RT107e

イーサアクセスVPNルーター

取扱説明書

ヤマハRT107eをお買い上げいただきありがとうございます。
お使いになる前に本書をよくお読みになり､正しく設置や設定を行ってください。
本書中の警告や注意を必ず守り、正しく安全にお使いください。
本書はなくさないように､大切に保管してください。

安全上のご注意

本製品を安全にお使いいただくために

以下の点を必ず守ってお使いください。

安全のための注意事項を守る

詳しくは、6～7ページをご覧ください。

故障したら使用を中止する。

お買い上げの販売店またはヤマハのお問い合わせ窓口(113ページ)にご連絡ください。

マークの意味

本書および本製品では、本製品を安全にお使いいただくため、守っていただきたい事項に次のマークを表示していますので、必ずお読みください。

⚠ 警告

人体に危険を及ぼしたり、装置に大きな損害を与える可能性があることを示しています。必ず守ってください。

⚠ 注意

機能停止を招いたり、各種データを消してしまう可能性があることを示しています。十分注意してください。

はじめにお読みください

お買い上げいただき、ありがとうございます。
本製品は中・小規模の企業ネットワークに適した、イーサアクセスVPNルーターです。

付属品をご確認ください

- LANケーブル（1本）
- 取扱説明書（本書）（1冊）
- CD-ROM（1枚）
- 保証書（1枚）

本書の主な内容

ご注意

- 本書は、本製品の基本的な機能を使用するための情報を提供するためのものです。
- 「コマンドリファレンス」（付属CD-ROMに収録）や、「かんたん設定ページ」のヘルプにはより詳細な情報が掲載されています。必要にあわせてご覧ください。

その他、本書には多くの情報が記載されています。詳しくは目次をご覧ください。

▶4 ページをご覧ください。

目次

はじめに

準備する

ネットワークに接続する

セキュリティを強化する

ルーターを使いこなす

ルーターの運用管理

困ったときは

付録

⚠警告

本製品を安全にお使いいただくために、下記のご注意をよくお読みになり、必ず守ってお使いください。

- 本製品は一般オフィス向けの製品であり、人の生命や高額財産などを扱うような高度な信頼性を要求される分野に適応するようには設計されていません。
  本製品を誤って使用した結果発生したあらゆる損失について、当社では一切その責任を負いかねますので、あらかじめご了承ください。
- 本製品から発煙や異臭がするとき、内部に水分や薬品類が入ったとき、および電源コードが発熱しているときは、直ちに電源コードをコンセントから抜いてください。そのまま使用を続けると、火災や感電のおそれがあります。
- 濡れた手で電源コードを触らないでください。感電や故障のおそれがあります。
- 電源コードを傷付けたり、無理に曲げたり、引っ張ったりしないでください。火災や感電、故障、ショート、断線の原因となります。
- 本製品の電源部は日本国内用AC100V（50/60Hz）の電源専用です。他の電源で使用すると、火災や感電、故障の原因となります。
- 安全のため、電源コードは容易に外すことのできるコンセントに接続してください。家具の後ろなど手の届かない場所にあるコンセントには接続しないでください。
- 本製品を落下させたり、強い衝撃を与えたりしないでください。内部の部品が破損し、感電や火災、故障の原因となります。
- 本製品を分解したり、改造したりしないでください。火災や感電、故障の原因となります。
- 本製品の通風口を塞いだ状態で使用しないでください。火災や感電、故障の原因となります。
- 電源を入れたままケーブル類を接続しないでください。感電や故障、本製品および接続機器の破損の恐れがあります。
- LANポート、ISDNポートなどの通信ポートには、本来接続される信号と異なる信号ケーブルを接続しないでください。火災や故障の原因となります。
- 本製品のポートに指や異物を入れないでください。感電や故障、ショートの原因となります。
- 本製品を他の機器と重ねて置かないでください。熱がこもり、火災や故障の原因となることがあります。
- 近くに雷が発生したときは、電源コードやケーブル類を取り外し、使用をお控えください。落雷によって火災や故障の原因となることがあります。
- 本製品に触れる際には、人体や衣服から静電気を除去する等、静電気対策を十分に行ってください。静電気によって故障する恐れがあります。

⚠注意

本製品を安全にお使いいただくために、下記のご注意をよくお読みになり、必ず守ってお使いください。

- 直射日光や暖房器等の風が当たる場所、温度や湿度が高い場所には、置かないでください。故障や動作不良の原因となります。
- 極端に低温の場所や温度差が大きい場所、結露が発生しやすい場所で使用しないでください。故障や動作不良の原因となります。結露が発生した場合は、電源コードをコンセントから抜き、乾燥させ、充分に室温に慣らしてから使用してください。
- ほこりが多い場所や油煙が飛ぶ場所、腐蝕性ガスがかかる場所、磁界が強い場所に置かないでください。故障や動作不良の原因となります。
- アースコードは必ず接続してください。感電防止やノイズ防止の効果があります。アース接続は必ず、電源コードをコンセントにつなぐ前に行ってください。また、アース接続をはずす場合は、必ず電源コードをコンセントから取りはずしてから行ってください。
- 本製品を修理や移動等の理由により輸送する場合には、必ず本製品の設定を保存してください。

使用上のご注意

- 本製品の使用方法や設定を誤って使用した結果発生したあらゆる損失について、当社では一切その責任を負いかねますので、あらかじめご了承ください。
- 本製品のご使用にあたり、周囲の環境によっては電話、ラジオ、テレビなどに雑音が入る場合があります。この場合は本製品の設置場所、向きを変えてみてください。
- 本製品を譲渡する際は、マニュアル類も同時に譲渡してください。
- 本製品を廃棄する場合には不燃物ゴミとして廃棄してください。または、お住まいの自治体の指示に従ってください。本製品はコイン型リチウム電池を内蔵しています。

重要なお知らせ

セキュリティ対策と本製品のファイアウォール機能について

インターネットを利用すると、ホームページで世界中の情報を集めたり、電子メールでメッセージを交換したりすることができ、とても便利です。その一方で、お使いのパソコンが世界中から不正アクセスを受ける危険にさらされることになります。
特にインターネットに常時接続したり、サーバを公開したりする場合には、不正アクセスの危険性を理解して、セキュリティ対策を行う必要があります。本製品はそのためのファイアウォール機能を装備していますが、不正アクセスの手段や抜け道(セキュリティホール)は、日夜新たに発見されており、それを防ぐ完璧な手段はありません。
インターネット接続には、常に危険がともなうことをご理解いただくとともに、常に新しい情報を入手し、自己責任でセキュリティ対策を行うことを強くおすすめいたします。

プロバイダ契約について

本製品をルーターとしてお使いになる前(または新たにプロバイダ契約を行う前)に、必ずルーター経由による複数パソコンの同時接続が、プロバイダによって禁止されていないかどうかご確認ください。**プロバイダによっては、禁止もしくは別の契約が必要な場合があります。契約に違反して本製品を使用すると、予想外の料金を請求される場合があります。**
禁止されている場合は、プロバイダと別途必要な契約を行うか、同時接続を禁止していない他のプロバイダと契約してください。

電波障害自主規制について

この装置は、情報処理装置等電波障害自主規制協議会(VCCI)の基準に基づくクラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

高調波について

JIS C 61000-3-2適合品
JIS C 61000-3-2適合品とは、日本工業規格「電磁両立性–第3-2部：限度値–高調波電流発生限度値(1相当たりの入力電流が20A以下の機器)」に基づき、商用電力系統の高調波環境目標レベルに適合して設計・製造した製品です。

輸出について

本製品は「外国為替及び外国貿易法」で定められた規制対象貨物(および技術)に該当するため、輸出または国外への持ち出しには、同法および関連法令の定めるところに従い、日本国政府の許可を得る必要があります。

本書の表記について

略称について

本書ではそれぞれの製品について、以下のように略称で記載しています。

- YAMAHA RT107e：本製品
- Microsoft® Windows®：Windows
- Microsoft® Windows XP®：Windows XP
- 10BASE-T（100BASE-TX)ケーブル：LANケーブル

設定例について

本書に記載されているIPアドレスやドメイン名、URLなどの設定例は、説明のためのものです。実際に設定するときは、必ずプロバイダから指定されたものをお使いください。

詳細な技術情報について

本製品を使いこなすためには、インターネットやネットワークに関する詳しい知識が必要となる場合があります。付属のマニュアルではこれらの情報について解説しておりませんので、詳しくは市販の解説書などを参考にしてください。

商標について

- イーサネットは富士ゼロックス社の登録商標です。
- Microsoft 、Windowsは米国Microsoft社の米国およびその他の国における登録商標です。
- Adobe 、Acrobatは米国Adobe Systems社の登録商標です。

DOWNLOADボタンご使用時のソフトウェアライセンス契約について

本製品の設定を変更することにより、DOWNLOADボタンを操作して、本製品の内蔵ファームウェアをリビジョンアップすることができます。

リビジョンアップを許可するように設定を変更する、および、DOWNLOADボタンを押してリビジョンアップを実行する、という操作は、ソフトウェアライセンス契約(以下「本契約書」)(次ページ参照)に同意したこととみなされます。ご使用になられる前に、必ず本契約書をお読みください。

本契約書の内容に同意していただけない場合には、DOWNLOADボタンの操作によるファームウェアのリビジョンアップを許可する設定に変更してはなりません。過失を含むいかなる場合であっても、ヤマハは、本使用許諾契約に起因するお客様側の損害について一切の責任を負いません。

なお、DOWNLOADボタンを使用しないでリビジョンアップする方法も提供しております。そちらをご利用される方はhttp://NetVolante.jpをご参照ください。

DOWNLOADボタンの詳しい操作方法は、本書96ページにてご確認ください。
本書はお使いになる方がなくさないように大切に保管してください。

ソフトウェアライセンス契約

1. 使用許諾

本使用許諾契約の定めにご同意いただくことによりダウンロード可能となるヤマハRT、RTX、ネットボランチシリーズ(以下、「本製品」という)用ファームウェア(以下、「本プログラム」という)はヤマハ株式会社(以下、「ヤマハ」という)がお客様に使用許諾するものです。本使用許諾契約は、ダウンロードした本プログラム及び本使用許諾契約に基づいて作成された複製物に適用されます。

2. 再配布の禁止

本プログラムは、本製品の機能アップグレードを目的とした場合に限りダウンロードすることができます。不特定多数の者によるアクセスが可能なウェブ・サイトなどにアップロード、掲示することはヤマハの許可を得た場合を除きできないものとします。

3. 複製物の作成

バックアップ目的及び、複数の本製品のアップグレードに必要な場合を除き、本プログラムの複製物の作成はできないものとします。

4. 逆コンパイル、リバースエンジニアリング、逆アセンブルの禁止

お客様は、本プログラム又はその一部を、逆コンパイルし、リバースエンジニアリングし、逆アセンブルし、修正し、再使用許諾し、頒布し、二次的著作物を創作しないものとします。

5. 責任の制限

過失を含むいかなる場合であっても、ヤマハは、本使用許諾契約に起因するお客様側の損害について一切の責任を負いません。

6. 外国為替法及び外国貿易法による規制

本プログラムは、「外国為替及び外国貿易法第25条第1項」に基づいて規制される技術(役務)に該当します。このため、本プログラム、及び本プログラムをインストールした本製品の日本国外への持ち出しには、日本政府による輸出許可が必要となる場合があります。また、本プログラムの、日本国内に住所を持たない人への提供にも、日本政府による許可が必要となる場合があります。

7. 日本に居住する人への限定提供

本プログラムは、日本国内に居住する法人または個人にのみ提供されるものとします。

8. 日本国法令の準拠

本使用許諾契約は、日本国の法令に準拠し、これに基づいて解釈されるものとします。

ヤマハルーター製品のお客様サポートについて（サポート規定）

ヤマハ株式会社はルーター製品を快適に、またその性能・機能を最大限に活かしたご利用が可能となりますように以下の内容・条件にてサポートをご提供いたします。

1. サポート方法

①FAQ、技術情報、設定例、ソリューション例等のWeb掲載
②電話でのご質問への回答
③お問い合わせフォームからのご質問への回答
④カタログ送付
⑤代理店・販売店からの回答
　ご質問内容によっては代理店・販売店へご質問内容を案内し、代理店・販売店よりご回答させていただく場合がありますので予めご了承のほどお願い致します。

2. サポート項目

①製品仕様について
②お客様のご利用環境に適した弊社製品の選定について
③簡易なネットワーク構成での利用方法について
④お客様作成のconfigの確認、及びlogの解析
⑤製品の修理について
⑥代理店または販売店のご紹介

3.免責事項・注意事項

①回答内容につきましては正確性を欠くことのないように万全の配慮をもって行いますが、回答内容の保証、及び回答結果に起因して生じるあらゆる事項について弊社は一切の責任を負うことはできません。
また、サポートの結果又は製品をご利用頂いたことによって生じたデータの消失や動作不良等によって発生した経済的損失、その対応のために費やされた時間的・経済的損失、直接的か間接的かを問わず逸失利益等を含む損失及びそれらに付随的な損失等のあらゆる損失について弊社は一切の責任を負うことはできません。
尚、これらの責任に関しては弊社が事前にその可能性を知らされていた場合でも同様です。但し、契約及び法律でその履行義務を定めた内容は、その定めるところを遵守するものと致します。

②ファームウェアの修正は弊社が修正を必要と認めたものについて生産終了後2年間行います。

③質問受付対応、修理対応は生産終了後5年間行います。

④実ネットワーク環境での動作保証、性能保証は行っておりません。

⑤期日・時間指定のサポート、及び海外での使用、日本語以外でのサポートは行っていません。

⑥お問い合わせの回答を行うにあたって、必要な情報のご提供をお願いする場合があります。情報のご提供がない場合は適切なサポートができない場合があります。

⑦再現性がない、及び特殊な環境でしか起きない等の事象に関しては、解決のための時間がかかったり適切なサポートが行えない場合があります。

⑧オンサイト保守・定期保守等は代理店にて有償にて行います。詳細な内容は代理店にご確認をお願い致します。

⑨他社サービス、他社製品、及び他社製品との相互接続に関してのサポートは弊社Web上に掲載している範囲に限定されます。

⑩やむを得ない事由によりヤマハルーターの返品・交換が生じた場合は、ご購入店経由となります。尚、交換、返品に際しましてはご購入店、ご購入金額を証明する証憑が必要となります。

⑪製品の修理は代理店・販売店経由で受付けさせて頂きます。弊社への直接持ち込みはできません。また、着払いでの修理品受付は致しておりません。発送は弊社指定の通常宅配便(国内発送のみ)にて行わせて頂きます。修理完了予定期間は変更になる場合がありますのでご了承のほどお願い致します。尚、保証期間中の無償修理(無償例外事項)等の詳細規定は保証書に記載しております。

⑫上記サポート規定は予告なく変更されることがあります。

RT107eでできること

本製品は中・小規模の企業ネットワークに適した、イーサアクセスVPNルーターです。

ブロードバンド対応

各種のブロードバンド回線用モデムなどと本製品のWANポートをLANケーブルで接続することで、FTTHやADSL、CATVなどのブロードバンド回線でインターネットなどに接続して使用できます。

ファイアウォール機能

静的／動的の2種類のフィルタによるパケットフィルタリング機能で、外部からの不正アクセスに対してセキュリティを強化できます。不正アクセスや攻撃を検出した場合にお知らせする、不正アクセス検知機能も搭載しています。

IPsecによるVPN

本製品はIPsecに対応しているため、インターネット（ブロードバンド）回線を利用したVPN（仮想プライベートネットワーク）を構築する場合でも、より安全にデータをやり取りできます。

かんたん操作

- 本製品は設定のためのホームページ「かんたん設定ページ」を内蔵していますので、パソコンのWebブラウザを使って本製品の基本的な設定を変更できます。
- DOWNLOADボタンを押すだけで、内蔵ソフトウェアをリビジョンアップ（バージョンアップ）できます。ご購入後に新しい機能が追加されても、最新の機能を利用できます。
- STATUSランプの状態を確認することで、プロバイダとの接続やIPsecによるVPN接続、IPIPによるトンネル接続において、接続先の機器との通信が不可能な状態になっていないか確認できます。

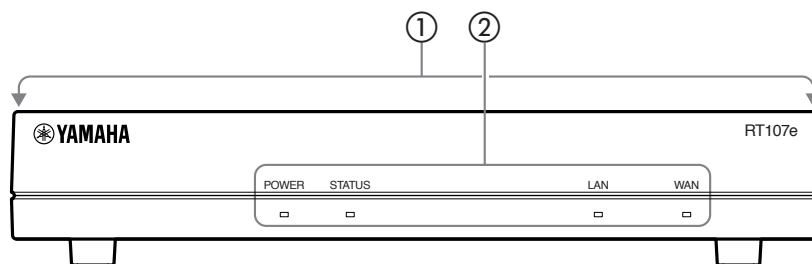
その他のルーター機能

- SNMP（Simple Network Management Protocol）に対応しています。RFC1157（SNMP）およびRFC1213（MIB-II）準拠の機能を搭載しています。
- 動的経路制御プロトコルRIPおよびRIP2、OSPF、BGP-4に対応しています。これらのプロトコル対応している他の機器との間で、経路情報をやり取りできます。
- VRRP（Virtual Router Redundancy Protocol）に対応しています。他のVRRP対応ルーターと併設することで、機器を冗長構成にすることができます。

充実のヤマハルーターホームページ

ヤマハルーターホームページ（http://NetVolante.jp/、http://www.rtpro.yamaha.co.jp/）で、ヤマハルーターを使った高度な活用例や詳しい解説がご覧いただけます。

各部の名称とはたらき

前面

① 通風口

内部の熱を逃がすための穴です。

② ランプ

本製品の動作状態を示します。

- **POWER：**本製品の電源の状態を示します。電源が入っているときは点灯します。
- **STATUS：**接続先の機器との通信が不可能な状態になっているかどうかを示します（95ページ）。
- **LAN：**LANポートの使用状態を示します。接続中は点灯、通信中は点滅します。
- **WAN：**WANポートの使用状態を示します。接続中は点灯、通信中は点滅します。

前面ランプの点灯状態

◉点灯　-◎- 点滅　◎消灯

POWERランプ

◉ 電源が入っています。
◎ 電源が切れているか、または停電しています。

STATUSランプ

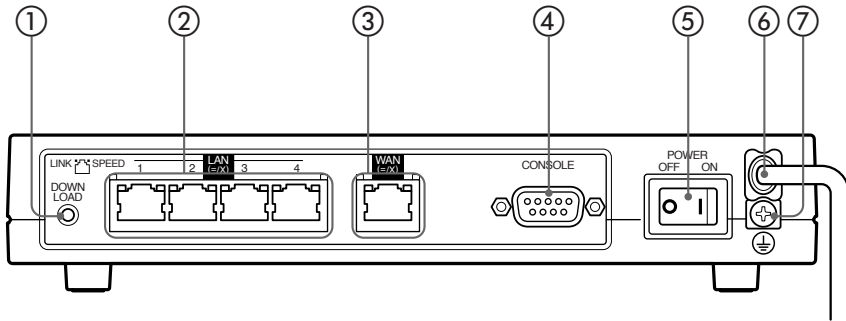
◉ 通信が不可能な状態になっています。
「STATUSランプが点灯しているときは」（95ページ）をご覧ください。
◎ 通信が不可能な状態になっていません。

LANランプ

◉ LANが使用可能な状態です。
-◎- LANにデータが流れています。
◎ LANが使用不可能な状態です。

WANランプ

◉ WANが使用可能な状態です。
-◎- WANにデータが流れています。
◎ WANが使用不可能な状態です。

背面

① DOWNLOADボタン

DOWNLOADボタンによるリビジョンアップを許可するように設定している場合は、このスイッチを3秒間押し続けるとファームウェアのリビジョンアップを開始します。詳しくは、「最新の機能を利用する(リビジョンアップ)」(96ページ)をご覧ください。

② LANポート

パソコンのLANポートまたはHUBのポートとLANケーブルで接続します。
各LANポートの上部には、LINKランプ(左側)とSPEEDランプ(右側)があります。

- **LINKランプ**：リンク状態によって、消灯(リンク喪失)または点灯(リンク確立)、点滅(データ転送中)します。
- **SPEEDランプ**:接続速度によって、消灯(10BASE-T接続)または点灯(100BASE-TX)します。

③ WANポート

ケーブルモデムやADSLモデム、ONUとLANケーブルで接続します。
WANポートの上部には、LINKランプ(左側)とSPEEDランプがあります。動作については、LANポートのランプと同様です。

④ CONSOLEポート

コンソールからの設定を行う場合に、パソコンのRS-232C端子(シリアルコネクタ)と接続します。詳しくは、「CONSOLEポートから設定する」(91ページ)をご覧ください。

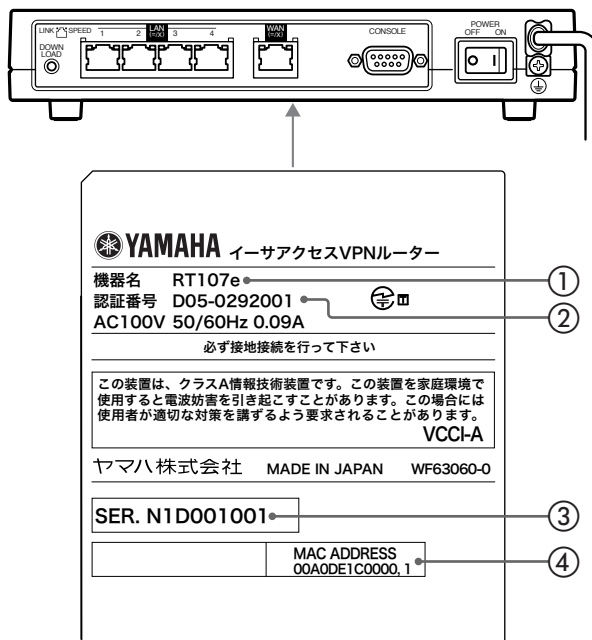
⑤ POWERスイッチ

本製品の電源を入／切します。

⑥ 電源コード

⑦ アース端子

アースコードを接続します。必ず接続してください。

底面

① 機器名

本製品の機器名が記載されています。

② 認証番号

本製品の認証番号が記載されています。

③ シリアル番号

製品を管理／区分するための製造番号です。

④ MACアドレス

LAN側とWAN側それぞれに付与されている機器固有のネットワーク識別番号が記載されています。「00A0DE1C0000, 1」という上図の例の場合、LAN側とWAN側それぞれのMACアドレスは以下のようになります。

- **LAN側MACアドレス：** 00A0DE1C0000
- **WAN側MACアドレス：** 00A0DE1C0001

準備の流れ

本製品を利用するには、以下の順序で準備を行う必要があります。

ネットワーク接続設定に必要な準備を行う

準備1	**本製品にパソコンや回線を接続して、電源を入れる**	▶20ページ
準備2	**「かんたん設定ページ」を開く**	▶22ページ
準備3	**本製品のパスワードを設定する**	▶24ページ
準備4	**本製品の日付・時刻を合わせる**	▶28ページ
準備5	**本製品のLAN側IPアドレスを設定する**	▶30ページ
準備6	**LAN内のパソコンのIPアドレスを変更する**	▶32ページ

ネットワーク接続を設定する

接続方法によって、設定に必要な手順が異なります。詳しくは「本製品の接続設定のしくみ」をご覧ください。 ▶36ページ

準備を始める前にご用意ください

アースコード

アースコードは必ず接続してください。感電防止やノイズ防止の効果があります。

LANケーブル

パソコンの台数や距離に合わせて、10BASE-Tまたは100BASE-TX対応のLANケーブルをご用意ください。

HUB

本製品のLANポートには、パソコンを4台まで直接接続できます。5台以上のパソコンを接続したい場合は、10BASE-Tまたは100BASE-TX対応のHUB（またはスイッチングHUBなど)をご用意ください。

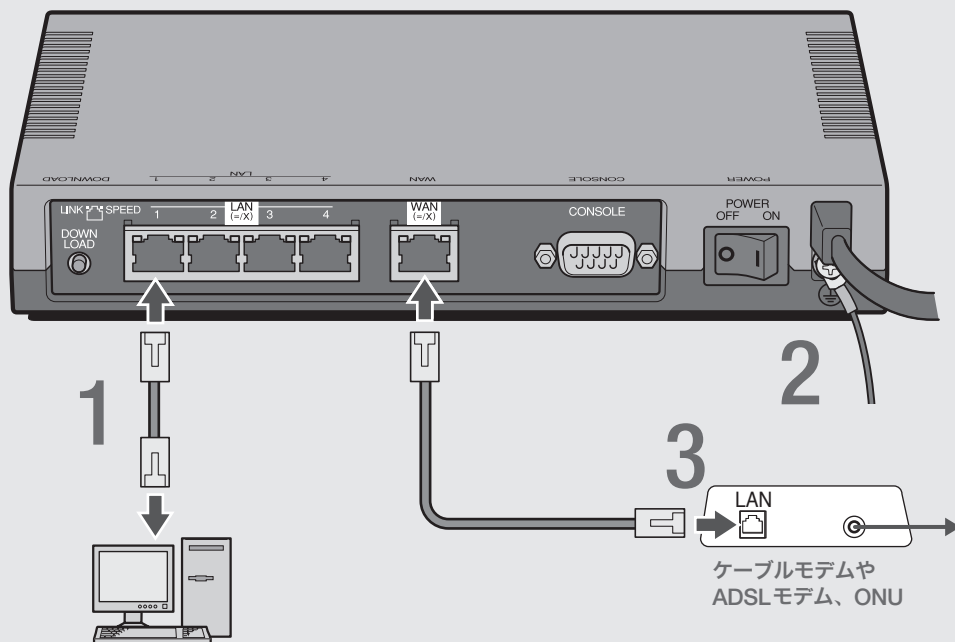
本製品を設置するネットワークの情報

本製品のLAN側に設定するIPアドレスを、あらかじめ決定しておいてください。

ご注意

DHCPサーバを使用しているLANに本製品を接続する場合は、本製品のDHCPサーバ機能を動作しないようにする必要があります。詳しくはネットワークの管理者にご相談ください。

準備 1

接続する

1 **パソコンのLANポートと本製品のLANポートを、LANケーブルで接続する。**

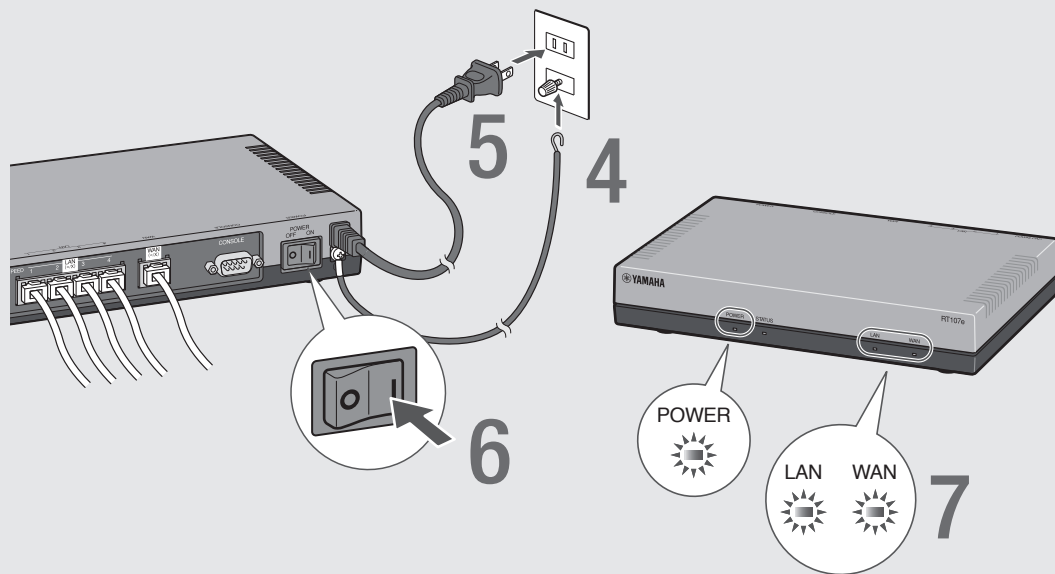
2 **アース端子のネジを+ドライバで少しゆるめてから、アースコードをアース端子に接続して固定する。**

アースコードは必ず接続してください。感電防止やノイズ防止の効果があります。

3 **ケーブルモデムやADSLモデム、ONUのLANポートと本製品のWANポートを、LANケーブルで接続する。**

プロバイダの資料やADSLモデム、ONUの取扱説明書もあわせてご覧ください。

ご注意

ケーブルモデムやADSLモデム、ONUとパソコンを直接接続している環境を本製品との接続に切り替えたり、設置されていたルータを本製品に置き換えた場合に、アドレスが取得できないなどの原因で正常接続できないことがあります。場合により、環境の変更後に何らかの設定やリセット操作、指定時間(例:20分以上)待つこと、などが必要となる場合があります。詳しくは、それらの取扱説明書の指示に従ってください。

4

アースコードをコンセントのアース端子へ接続する。

ご注意

アースコードは必ずコンセントのアース端子に接続してください。ガス管などには、絶対に接続しないでください。

5

本製品の電源コードをコンセントに接続する。

電源コードを取りはずす場合は

先に電源コードを取りはずしてから、アースコードを取りはずしてください。

6

本製品のPOWER（電源）スイッチを「ON」にして、電源を入れる。

ランプが何回か点滅した後、POWERランプが点灯します。

7

パソコンやHUBの電源を入れる。

本製品のLANランプとWANランプが点灯または点滅すれば正常です。

LANランプが点灯または点滅しない場合は

- LANケーブルが正しく接続されているかどうか、パソコンやHUBの電源が入っているかどうか確認してください。
- 本製品に接続したすべてのパソコンおよびHUBの電源が入っていないときは、LANランプは点灯または点滅しません。

WANランプが点灯または点滅しない場合は

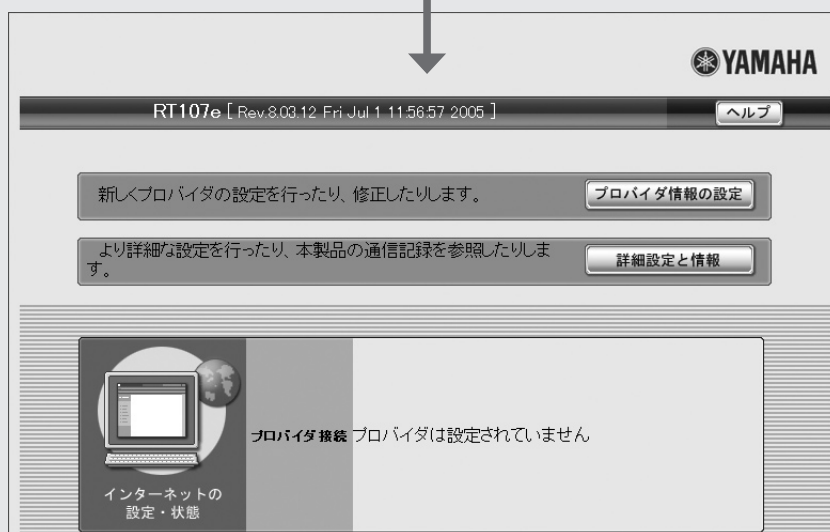
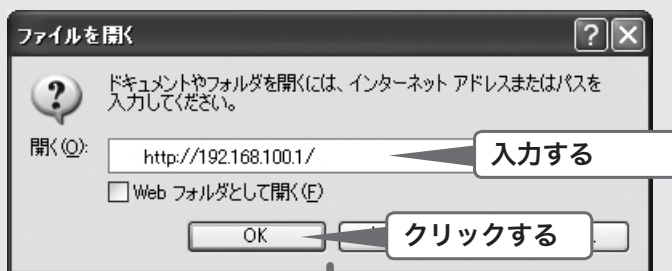
本製品とADSLモデム（またはケーブルモデムやONU）が正しく接続されているかどうか、ADSLモデム（またはケーブルモデムやONU）の電源が入っているかどうか確認してください。

準備 2

「かんたん設定ページ」を開く

本製品の設定の変更は、本製品に接続したパソコンのWebブラウザから本製品の「かんたん設定ページ」を開いて行います。
「かんたん設定ページ」を開くには、以下の手順で操作します。

ご注意
「かんたん設定ページ」を使用するには、Windows版Internet Explorer 6.0以降のWebブラウザが必要です。

ヒント
TELNETソフトウェアでコンソール画面からコマンドを入力して、「かんたん設定ページ」よりも詳細な設定を行うことができます(コンソールコマンド)。TELNETソフトウェアで本製品に接続する方法については88ページ、本製品で使用できるコマンドについては「コマンドリファレンス」(付属CD-ROMに収録)をご覧ください。

1 本製品の電源が入っていることを確認する。

2 パソコンでWebブラウザを起動して、「ファイル」メニューから「開く」を選ぶ。

3 「http://192.168. 100.1/」と半角英字で入力してから、「OK」をクリックする。

「かんたん設定ページ」のトップページが表示されます。

「かんたん設定ページ」のトップページが表示されないときは

「『かんたん設定ページ』で設定できない」(101ページ)をご覧ください。

「かんたん設定ページ」の見かた

パスワードを設定する

工場出荷状態では本製品にパスワードが設定されていません。セキュリティ対策を行う上でも、パスワードを設定することをおすすめします。パスワードを設定すると、本製品にアクセスする際にパスワード入力が必要となるので、第三者が本製品の設定を変更することが困難になります。

1

「かんたん設定ページ」のトップページの「詳細設定と情報」をクリックする。

「詳細設定と情報」画面が表示されます。

2

「ユーザとアクセス制限の設定(HTTP、TELNET、SSH)」の「設定」をクリックする。

「ユーザとアクセス制限の設定」画面が表示されます。

3

「管理パスワード」欄に本製品のパスワードを入力する。

入力したパスワードの文字は、●で表示されます。

4

「設定の確定」をクリックする。

設定したパスワードが有効になり、確認画面が表示されます。

5

「トップへ戻る」をクリックする。

パスワード入力画面が表示されます。

6

手順3で入力した本製品のパスワードを「パスワード」欄に入力してから、「OK」をクリックする。

「かんたん設定ページ」のトップページに戻ります。

ヒント

「ユーザー名」欄には、何も入力する必要はありません。

YAMAHA
RT107e [Rev.8.03.40 Wed Apr 19 20:20:41 2006]
ヘルプ
新しくプロバイダの設定を行ったり、修正したりします。
プロバイダ情報の設定
より詳細な設定を行ったり、本製品の通信記録を参照したりします。
詳細設定と情報
7 クリックする
IPv6の設定
UPnPの設定
LANの設定(IPアドレス、DHCPサーバ)
本体の設定(日付・時刻)
ユーザとアクセス制限の設定(HTTP、TELNET、SSH)
DOWNLOADボタンの設定
設定
8 クリックする
詳細設定と情報
ユーザとアクセス制限の設定
ユーザとパスワードの設定
ユーザの登録数: 1
無名ユーザ
管理パスワード
管理パスワードを設定すると、かんたん設定にログインするときに必要になります。
同じものをもう一度
管理パスワードを暗号化して保存する
9 クリックする
無名ユーザの設定
ログインパスワード
ログインパスワードを暗号化して保存する
10 入力する
コマンドによる管理ユーザへの昇格
許可する 許可しない
コネクションの制限
全ての接続を許可する
全ての接続を禁止する
接続方法ごとに許可する
シリアルコンソールからの接続を許可する
TELNETによる接続を許可する
接続の許可
すべて許可する
IPアドレス指定
設定の確定
11 クリックする
トップへ戻る

7 「かんたん設定ページ」のトップページの「詳細設定と情報」をクリックする。

「詳細設定と情報」画面が表示されます。

8 「ユーザとアクセス制限の設定(HTTP、TELNET、SSH)」の「設定」をクリックする。

「ユーザとアクセス制限の設定」画面が表示されます。

9 「ユーザとパスワードの設定」欄の「無名ユーザ」の「設定」をクリックする。

「無名ユーザの設定」画面が表示されます。

10 「ログインパスワード」欄にログイン用のパスワードを入力する。

入力したパスワードの文字は、●で表示されます。

11 「設定の確定」をクリックする。

設定したパスワードが有効になり、確認画面が表示されます。

12 「トップへ戻る」をクリックする。

「かんたん設定ページ」のトップページに戻ります。

準備 4

日付・時刻を合わせる

「本体の設定」画面で、本製品の日付と時刻を合わせます。

1 「かんたん設定ページ」のトップページの「詳細設定と情報」をクリックする。

「詳細設定と情報」画面が表示されます。

2 「本体の設定（日付・時刻）」の「設定」をクリックする。

「本体の設定」画面が表示されます。

3 「日付と時刻の設定」欄の、「下記設定日時に変更する」にチェックを付ける。

4 日付と時刻を入力する。

ヒント

あらかじめ少し先の時刻を入力しておき、時報と同時に「設定の確定」をクリックするとより正確に時刻合わせできます。

5 「設定の確定」をクリックする。

確認画面が表示されます。

6 「トップへ戻る」をクリックする。

「かんたん設定ページ」のトップページに戻ります。

本製品の時刻を自動的に合わせたいときは

インターネット上のNTPサーバ(時刻配信サーバ)を利用して、本製品の時刻を自動的に合わせることができます。また、NTPサーバを利用して手動で時刻を合わせたり、時刻を直接入力して合わせたりすることもできます。
詳しくは、「本体の設定」画面のヘルプをご覧ください。

ご注意

- 本製品のセキュリティ設定によっては、本製品だけでなくLAN内のパソコンからもNTPサーバを利用して時刻を合わせられない場合があります。外部のNTPサーバを利用する場合は、フィルタの設定を変更してください(70ページ)。
- ファイアウォール機能のセキュリティレベルが4または5（静的セキュリティフィルタ)に設定されている場合は、NTPサーバからの応答パケットが破棄されてしまうため、時刻を合わせることができません。
  この方法で時刻を合わせるときは、ファイアウォール機能のセキュリティレベルを6または7（動的セキュリティフィルタ)に設定してください(70ページ)。

準備 5

LAN側IPアドレスを設定する

ブロードバンド回線を経由して異なる場所のLAN同士を接続する場合は、それぞれのLANのネットワークアドレスが重複しないようにする必要があります。それぞれのLANの新たなネットワークアドレスを決めて、本製品とパソコンに新たなネットワークアドレスに応じたIPアドレスとネットマスクを設定してください。

ご注意

すでに異なるネットワークアドレスが設定されている場合には、そのネットワークアドレスに応じたIPアドレスとネットマスクを本製品に設定してください。本製品には、LAN内にすでに設置されている他の機器のIPアドレスと重複しないIPアドレスを設定してください。

1 「かんたん設定ページ」のトップページの「詳細設定と情報」をクリックする。

「詳細設定と情報」画面が表示されます。

2 「LANの設定（IPアドレス、DHCPサーバ）」をクリックする。

「LANの設定」画面が表示されます。

3 「LANポートのIPアドレス設定」欄に、本製品のLAN側IPアドレスを入力する。

プライマリ・IPアドレス
新たに決めたネットワークアドレスに応じたIPアドレスとネットマスクを入力する。

4 「DHCPサーバ機能」欄に、LAN内のパソコンに割り当てるIPアドレスを入力する。

IPアドレスの割り当て範囲
本製品のIPアドレスとは重複しないように、割り当てるIPアドレスの範囲を入力します。
ネットマスクビット数には、本製品のネットマスクと同じ値を入力します。

5 「設定の確定」をクリックする。

確認画面が表示されます。

6 「実行」をクリックしてから、パソコンのIPアドレスを変更する。

パソコンのIPアドレスを変更するには、次ページからの説明をご覧ください。

準備 6

LAN内のパソコンのIPアドレスを変更する

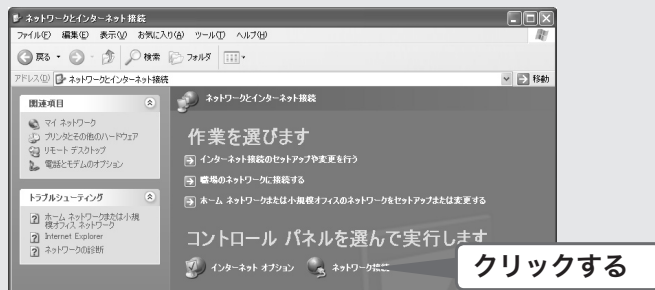
LANのネットワークアドレスを変更した場合には、本製品以外にもLAN内のパソコンのIPアドレスとネットマスクも変更する必要があります。なお、LAN内にパソコン以外の機器も設置されている場合には、それらの機器のIPアドレスとネットマスクもあわせて変更する必要があります。それらの機器の設定方法については、各機器の取扱説明書をご覧ください。

ご注意

- 本製品を設置したLANのネットワークアドレスを変更していない場合は、LAN内のパソコンのIPアドレスを変更する必要はありません。
- 本製品とパソコンのIPアドレスとネットマスクを変更した後は、「かんたん設定ページ」を開くには「http://192.168.100.1/」ではなく、「http://本製品の新たなIPアドレス/」を指定します。

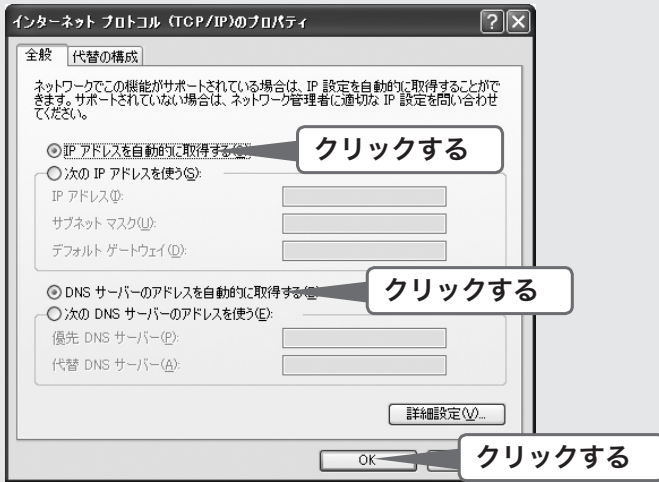
1 「スタート」ボタンをクリックして、「コントロール パネル」をクリックする。

2 「ネットワークとインターネット接続」をクリックする。

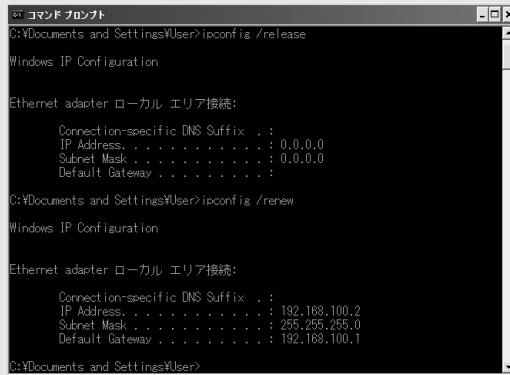
3 「ネットワーク接続」をクリックする。

4 「ローカルエリア接続」のアイコンをクリックする。

5 「この接続の設定を変更する」をクリックする。

6 「インターネットプロトコル(TCP/IP)」を選んでから、「プロパティ」をクリックする。

7 「IPアドレスを自動的に取得する」と「DNSサーバーのアドレスを自動的に取得する」を選んでから、「OK」をクリックする。

8 「ローカルエリア接続のプロパティ」画面で「OK」をクリックする。

9 「スタート」ボタンをクリックして、「すべてのプログラム」–「アクセサリ」–「コマンド プロンプト」をクリックする。

10 「ipconfig /release」と入力してから、Enterキーを押す。

パソコンに割り当てられていたIPアドレスが解放されます。

11 「ipconfig /renew」と入力してから、Enterキーを押す。

新たなIPアドレスがパソコンに割り当てられます。

12 LAN上のすべてのパソコンに対して手順1〜8の操作を繰り返し、すべてのパソコンが異なるIPアドレスを持つように設定する。

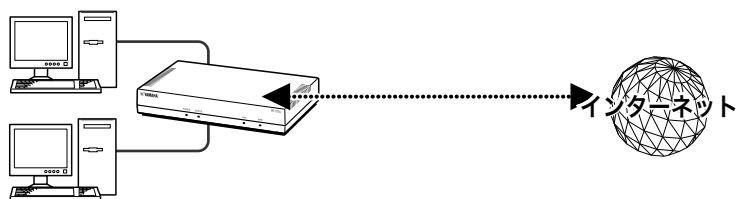
本製品の接続設定のしくみ

本書で説明している接続設定の種類と、接続設定ごとに必要な本書の説明ページを説明します。

本書で説明する接続設定

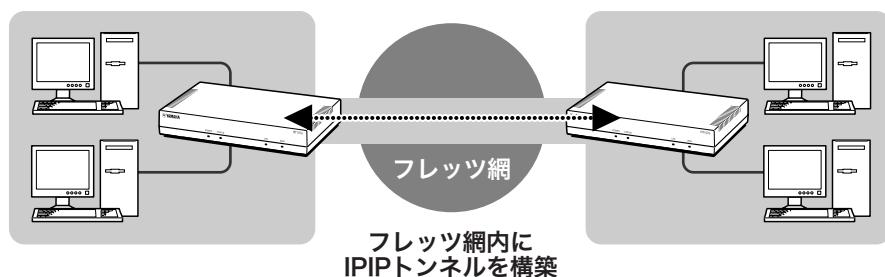
本書では、次の3通りの接続設定について説明しています。

① 基本的なインターネット接続

CATVインターネットやPPPoEを用いない端末型ADSL接続、およびPPPoEを用いる端末型ADSL接続（フレッツ・ADSL、Bフレッツ）で、インターネットに接続します。

② IPsec接続

IPsecでIPパケットデータを暗号化した状態でデータをやり取りする、仮想プライベートネットワーク（VPN）を構築します。

③ IPIPトンネル接続

NTT東日本の「フレッツ・グループアクセス ライト」やNTT西日本の「フレッツ・グループ ベーシックメニュー」のように、固定IPアドレスが1つだけ払い出される契約（端末型払い出し）でフレッツ網に接続して、IPIPトンネルでLAN同士を接続します。

利用する接続方法により、必要な設定が異なります

利用する接続設定ごとに、参照する必要のある説明ページが異なります。以下の説明をご覧になり、導入環境に適した場合の説明をご覧ください。

「① 基本的なインターネット接続」を利用する場合

- 「接続1：インターネットへ接続する（PPPoE/CATV）」の説明に従って、接続設定を行います。▶38ページ
- この設定が終われば、それ以外の設定を行う必要はありません。

「② IPsec接続」を利用する場合

- まず、「接続1：インターネットへ接続する（PPPoE/CATV）」の説明に従って、基本的なインターネット接続設定を行います。▶38ページ
- 引き続き、「IPsecでVPNを構築する」の説明に従って、IPsec通信に必要な接続設定を行います。▶48ページ

「③ IPIPトンネル接続」を利用する場合

使用方法によって異なります。

IPIPトンネル接続のみを使用する場合

NTT東日本の「フレッツ・グループアクセス ライト」やNTT西日本の「フレッツ・グループ ベーシックメニュー」を使用して、別の拠点とのIPIPトンネル通信専用として本製品を使用する場合です。

- 「接続3:フレッツ網を使用して、LAN同士をIPIPトンネル接続する」の説明に従って、IPIPトンネル通信に必要な接続設定を行います。▶55ページ
- この設定が終われば、それ以外の設定を行う必要はありません。

IPIPトンネル接続以外に、インターネット接続も行う場合

別の拠点とのIPIPトンネル通信以外に、インターネットへの接続ゲートウェイとしても本製品を使用する場合です。

- まず、「接続1：インターネットへ接続する（PPPoE/CATV）」の説明に従って、基本的なインターネット接続設定を行います。▶38ページ
- 引き続き、「接続3：フレッツ網を使用して、LAN同士をIPIPトンネル接続する」の説明に従って、IPIPトンネル通信に必要な接続設定を行います。▶55ページ

接続 1

インターネットへ接続する（PPPoE/CATV）

通常の方法でインターネットに接続するための設定を行います。

設定する前に

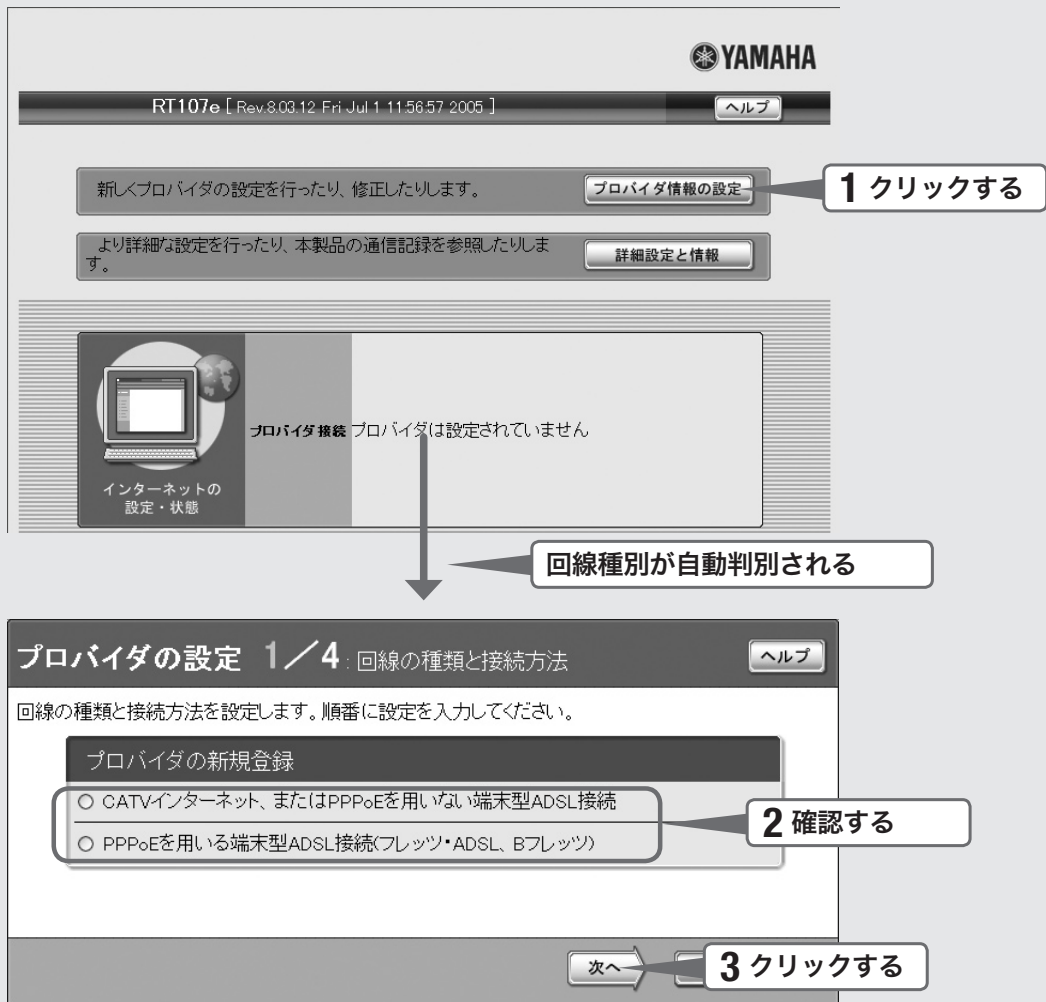
ご注意

- プロバイダ契約を解除または変更した時は、必ず本製品の接続設定を削除または再設定してください。削除しないまま使っていると、回線業者やプロバイダから意図しない料金を請求される場合があります。
- インターネットへ常時接続する場合は、インターネット側から不正なアクセスや攻撃を受ける危険性が高くなります。セキュリティには十分ご注意の上、お使いください。詳しくは「セキュリティを強化する」(66ページ)をご覧ください。

プロバイダの設定資料を用意してください

接続先を設定してインターネットに接続するには、プロバイダから通知される以下の情報が必要です（接続方法によっては、必要のないものもあります）。

- ユーザID（認証ID、アカウント名）
- パスワード（認証パスワード、初期パスワード）
- IPアドレス
- ネットマスク
- ネームサーバアドレス（DNSサーバアドレス、ネームサーバIPアドレス、DNSサーバIPアドレス）
- デフォルト・ゲートウェイ・アドレス

1　接続方法を確認する

1　「かんたん設定ページ」のトップページで、「プロバイダ情報の設定」をクリックする。

本製品のブロードバンド回線自動判別機能が動作して、接続した回線に合わせた接続方法が選ばれた画面が表示されます。

ご注意

- 本製品のWANポートにブロードバンド回線を接続していない場合は、自動判別機能は動作しません。
- 回線自動判別機能を一度実行すると、次回から自動判別は行いません。

2 自動判別された接続方法を確認する。

A 「CATVインターネット、またはPPPoEを用いない端末型ADSL接続」が選ばれた場合

プロバイダの新規登録

◉ CATVインターネット、またはPPPoEを用いない端末型ADSL接続

○ PPPoEを用いる端末型ADSL接続(フレッツ・ADSL、Bフレッツ)

「CATVインターネット、またはPPPoEを用いない端末型ADSL接続」が選ばれる代表的な接続サービスは、以下の通りです。

- Yahoo! BB
- アッカ・ネットワークス(ADSLモデムがルータモードの場合)
- イー・アクセス(ADSLモデムがルータモードの場合)
- プロバイダ独自のADSL接続サービス
- 各種CATVインターネット接続サービス

B 「PPPoEを用いる端末型ADSL接続(フレッツ・ADSL、Bフレッツ)」が選ばれた場合

プロバイダの新規登録

○ CATVインターネット、またはPPPoEを用いない端末型ADSL接続

◉ PPPoEを用いる端末型ADSL接続(フレッツ・ADSL、Bフレッツ)

「PPPoEを用いる端末型ADSL接続(フレッツ・ADSL、Bフレッツ)」が選ばれる代表的な接続サービスは、以下の通りです。

- フレッツ・ADSL
- Bフレッツ
- アッカ・ネットワークス(ADSLモデムがブリッジモードの場合)
- イー・アクセス(ADSLモデムがブリッジモードの場合)

何も選ばれなかった場合は

▶ブロードバンド回線の自動判別に失敗しました。

接続回線に合わせて「CATVインターネット、またはPPPoEを用いない端末型ADSL接続」または「PPPoEを用いる端末型ADSL接続(フレッツ・ADSL、Bフレッツ)」を選んでから、「次へ」をクリックしてください。

どちらかわからない場合は、契約書を確認するかプロバイダにお問い合わせください。

3 「次へ」をクリックする。

接続回線に合わせた設定画面が表示されます。

以下の設定は接続回線によって異なりますので、選んだ接続回線の説明をご覧ください。

A 「CATVインターネット、またはPPPoEを用いない端末型ADSL接続」が選ばれた場合 ▶41 ページをご覧ください。

B 「PPPoEを用いる端末型ADSL接続(フレッツ・ADSL、Bフレッツ)」が選ばれた場合 ▶44 ページをご覧ください。

A CATVインターネット（40ページから） 2—プロバイダの情報を指定する

1 設定名を入力する。

接続先がわかるような名前を入力します。名前は自由に付けられますが、あとで設定を修正する必要が出たときなどにわかりやすい名前にしておくと便利です。

2 WAN側IPアドレスを指定する。

プロバイダからIPアドレスが指定されていない場合

「DHCPクライアント」をクリックして選びます。
プロバイダからDHCPクライアント識別名を指定されている場合は、「DHCPクライアント識別名」欄に指定された識別名を入力します（指定されていない場合は、入力する必要はありません）。

プロバイダからIPアドレスを指定されている場合

「指定IPアドレス」をクリックして選んでから、以下の設定を行います。

- **WAN側IPアドレス：**プロバイダから指定されたIPアドレスを、半角数字で入力します。
- **ネットマスク：**プロバイダから指定されたネットマスクを選びます。
- **デフォルトゲートウェイ：**プロバイダから指定されたデフォルト・ゲートウェイ・アドレスを、半角数字で入力します。

3 「次へ」をクリックする。

「プロバイダの設定3/4」画面が表示されます。

A CATVインターネット

3—DNSサーバアドレスを指定する

1 DNSサーバアドレスを指定する。

プロバイダからDNSサーバアドレスが指定されていない場合
「DNSサーバアドレスを指定しない、またはプロバイダから自動取得」をクリックして選びます。

プロバイダからDNSサーバアドレスが指定されている場合
「プロバイダとの契約書にDNSサーバアドレスの指定がある」をクリックして選んでから、以下の設定を行います。

- **プライマリDNSサーバアドレス：**プロバイダから指定されているDNSサーバアドレスを半角数字で入力します。
- **セカンダリDNSサーバアドレス：**プロバイダから指定されているDNSサーバアドレスが2つある場合に入力します(1つだけ指定されている場合は、この欄は空欄にしてください)。

2 「次へ」をクリックする。

「プロバイダの設定4/4」画面が表示されます。

A CATVインターネット

4―設定内容を確認して、インターネットに接続する

プロバイダの設定 4／4：設定内容の確認　ヘルプ

設定内容の確認後、[設定の確定] ボタンを押してください。

プロバイダの新規登録	
接続型	CATVインターネット、またはPPPoEを用いない端末型ADSL接続
設定名	CATV
WAN側IPアドレス	自動取得
DNSサーバアドレス	自動取得

1 確認する

戻る　設定の確定

2 クリックする

インターネットの設定・状態　プロバイダ接続　WANポート CATV　通信中　グローバル 000.000.000.000/23

3 確認する

1 表示された設定内容が、プロバイダから送付された設定資料と合っているかどうか確認する。

誤って設定した内容がある場合は、「戻る」をクリックして必要な設定画面を表示して、正しく設定し直してください。

2 「設定の確定」をクリックする。

表示された確認画面で「トップへ戻る」をクリックすると、本製品は自動的にインターネットに接続して「かんたん設定ページ」のトップページに戻ります。

3 インターネットに接続しているかどうか確認する。

画面下部の表示を見て、本製品がインターネットに接続していることを確認してください。

設定終了

これでインターネットへの接続設定は終了です

▶インターネットに接続できない場合は

Check 1　本製品とパソコン、ADSLモデムやケーブルモデムの接続を確認してください。

Check 2　41～42ページの設定内容をもう一度確認してください。

Check 3　それでも問題が解決しない場合は、「困ったときは」を参考にして、問題を解決してください。

2―プロバイダの情報を指定する

1 設定名を入力する。

接続先がわかるような名前を入力します。名前は自由に付けられますが、あとで設定を修正する必要が出たときなどにわかりやすい名前にしておくと便利です。

2 ユーザIDを入力する。

プロバイダから指定された、接続用のユーザIDを入力します。必ず書類を確認して、間違いのないように入力してください。

ご注意

フレッツ・ADSLやBフレッツで接続する場合は、ユーザIDの後にプロバイダ名を入力する必要があります。詳しくはフレッツ・ADSLまたはBフレッツの契約の際にNTTから送付された資料や、プロバイダからの資料をご覧ください。
ユーザIDがusernameの場合の例：
username@provider.ne.jp
username@aaa.provider.ne.jp（サブドメインが付加される場合）

3 接続パスワードを入力する。

プロバイダから指定されたパスワード（または自分で変更したパスワード）を入力します。半角英数字で、大文字小文字も正確に入力してください。
入力したパスワードの文字は●で表示されます。

4 「次へ」をクリックする。

「プロバイダの設定3/4」画面が表示されます。

B PPPoE端末型 3—DNSサーバアドレスを指定する

1 DNSサーバアドレスを指定する。

プロバイダからDNSサーバアドレスが指定されていない場合

「DNSサーバアドレスを指定しない、またはプロバイダから自動取得」をクリックして選びます。

プロバイダからDNSサーバアドレスが指定されている場合

「プロバイダとの契約書にDNSサーバアドレスの指定がある」をクリックして選んでから、以下の設定を行います。

- **プライマリDNSサーバアドレス：**プロバイダから指定されているDNSサーバアドレスを半角数字で入力します。
- **セカンダリDNSサーバアドレス：**プロバイダから指定されているDNSサーバアドレスが2つある場合に入力します(1つだけ指定されている場合は、この欄は空欄にしてください)。

2 「次へ」をクリックする。

「プロバイダの設定4/4」画面が表示されます。

B PPPoE端末型 4―設定内容を確認する

1 表示された設定内容が、プロバイダから送付された設定資料と合っているかどうか確認する。

誤って設定した内容がある場合は、「戻る」をクリックして必要な設定画面を表示して、正しく設定し直してください。

2 「設定の確定」をクリックする。

「プロバイダの登録」画面が表示されます。

B PPPoE端末型 5―インターネットに接続する

1 「接続」をクリックする。

インターネットに接続して、「プロバイダへの接続・切断」画面が表示されます。
「トップへ戻る」をクリックすると、「かんたん設定ページ」のトップページに戻ります。

2 インターネットに接続しているかどうか確認する。

画面下部の表示を見て、本製品がインターネットに接続していることを確認してください。

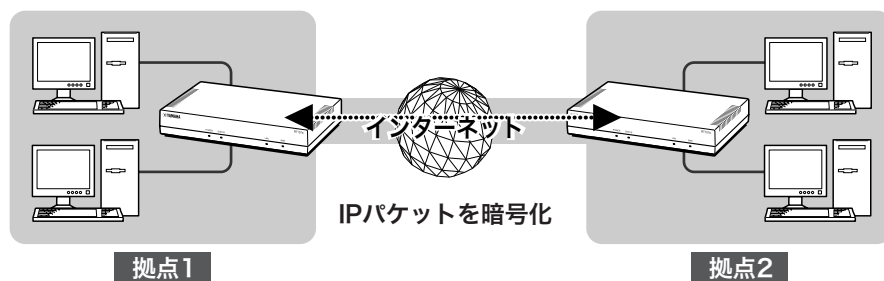
設定終了

これでインターネットへの接続設定は終了です

▶インターネットに接続できない場合は

Check 1　本製品とパソコン、ADSLモデムやONUの接続を確認してください。
Check 2　44～46ページの設定内容をもう一度確認してください。
Check 3　それでも問題が解決しない場合は、「困ったときは」を参考にして、問題を解決してください。

IPsecでVPNを構築する

IPsecを利用するとIPパケットを暗号化した状態でやり取りできるため、セキュリティを保った状態でインターネット経由でLAN同士を接続できます（仮想プライベートネットワーク、VPN）。ADSLなどの通常のブロードバンド回線をそのまま利用してVPNを構築できるため、専用線を導入する場合と比較して、低コストでVPNを実現できます。

本製品で利用できるIPsecについて

- 鍵交換プロトコルはIKE（Internet Key Exchange）を使用します。必要な鍵はIKEにより自動的に生成されますが、鍵の種となる事前共有鍵をあらかじめ登録しておく必要があります（ipsec ike pre-shared-keyコマンド）。
- 鍵や鍵の寿命、暗号や認証のアルゴリズムなどを登録した管理情報は、SA（Security Association）で管理します。
- セキュリティ・ゲートウェイとなる、相手機器のプログラムのリビジョンにご注意ください。IPsecリリース2とIPsecリリース3には相互接続性がありますが、後者の設定を前者に合わせる必要があります。なお、本製品で利用できるセキュリティ・ゲートウェイの識別子は1〜6、トンネルインタフェース番号も同様に1〜6となります。
- 本製品はメインモードとアグレッシブモードに対応していますが、モードを自由に選択することはできません。
  - VPNを構成する両方のルータが固定グローバルIPアドレスを持つ場合はメインモード、一方のルータのみ固定グローバルIPアドレスを持つ場合（ダイヤルアップVPNなど）はアグレッシブモードを使用します。
  - メインモードを使用する場合は、対向のルータのIPアドレスを設定する必要があります。
  - アグレッシブモードを使用する場合は、固定のグローバルIPアドレスを持つかどうかによって、設定が異なります。
- 本製品のIPsecの仕様および設定コマンドについて詳しくは、「コマンドリファレンス」（付属CD-ROMに収録）をご覧ください。

IPsecには2種類の通信モードがあります

IPsecによる通信には、大きく分けてトンネルモードとトランスポートモードの2種類があります。トンネルモードとトランスポートモードは併用が可能ですが、それぞれを二重に適用することはできません。

トンネルモード

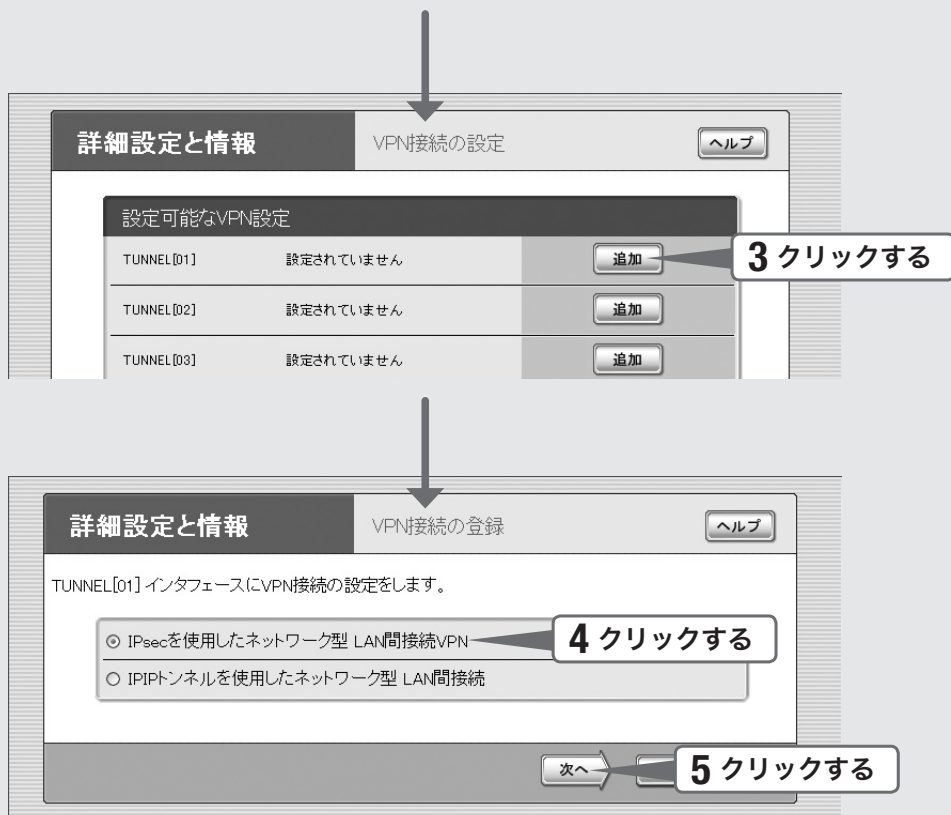
IPsec によるVPNを利用するための通信モードです。ルータがセキュリティ・ゲートウェイとなり、LAN上に流れるIPパケットデータを暗号化して、対向のセキュリティ・ゲートウェイとの間でデータをやりとりします。ルータがIPsecに必要な処理をすべて行うので、LAN上の始点や終点となるホストには特別な設定を必要としません。
トンネルモードを使用する場合は、「トンネルインタフェース」という仮想的なインタフェースを定義し、処理すべきIPパケットがトンネルインタフェースに流れるように経路を設定します。個々のトンネルインタフェースは、トンネルインタフェース番号で管理されます。

トランスポートモード

ルータ自身が始点または終点になる通信に対してセキュリティを保証する、特殊な通信モードです。ルータからリモートのルータへtelnetでアクセスするなどの特殊な場合に利用できます。

1. 接続方法を指定する

本製品でIPsec通信するために必要な設定を行います。
インターネットに接続するための設定をしていない場合は、「接続1:インターネットへ接続する(PPPoE/CATV)」(38ページ)の設定を行ってインターネットに接続できるようにしてから、以下の設定を行ってください。

ネットワークに接続する

1 「かんたん設定ページ」のトップページの「詳細設定と情報」をクリックする。

「詳細設定と情報」画面が表示されます。

2 「VPN接続の設定」の「設定」をクリックする。

「VPN接続の設定」画面が表示されます。

3 登録したい接続先の「追加」をクリックする。

「VPN接続の登録」画面が表示されます。

4 「IPsecを使用したネットワーク型LAN間接続VPN」を選ぶ。

5 「次へ」をクリックする。

「VPN接続設定の登録/修正」画面が表示されます。

2. IPsec接続に必要な情報を指定する

ネットワークに接続する

1 「設定名」欄で、設定名を入力する。

接続先がわかるような名前を入力します。名前は自由に付けられますが、あとで設定を修正する必要が出たときなどにわかりやすい名前にしておくと便利です。

2 認証鍵を入力する。

データの暗号化に使用する事前共有鍵(半角英数字で最大32文字)を入力します。
センター側と拠点側で同じ値に設定してください。

3 接続先の識別方法を指定する。

IPアドレスで識別する場合

- 「IPアドレスで識別」を選んでから、接続先のIPアドレスを入力します。
- 設定しているルーターに固定IPアドレスが割り当てられていない場合は、「自分の名前を通知する」にチェックを付けてから自分の名前を入力します。

名前で識別する場合

「名前で識別」を選んでから、接続先の名前(半角英数字で最大32文字)を入力します。

4 認証アルゴリズムを指定する。

- IKEのフェーズ2で使用する、認証に使用するアルゴリズムを設定します。
- 接続先のルーターと同じ設定にしてください。

5 暗号アルゴリズムを指定する。

- IKEのフェーズ2で使用する、暗号化に使用するアルゴリズムを設定します。
- 接続先のルーターと同じ設定にしてください。

6 経路情報を指定する。

接続先のLANのネットワークアドレスを設定します。

ご注意

双方でネットワークアドレスが重複している場合は、どちらかのネットワーク アドレスを変更してください。

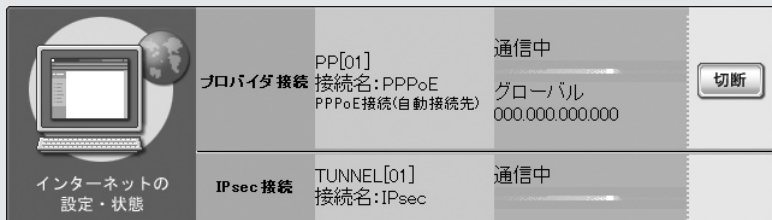
7 「設定の確定」をクリックする。

接続相手が登録され、確認画面が表示されます。

8 「トップへ戻る」をクリックする。

「かんたん設定ページ」のトップページに戻ります。

3. IPsec接続する

センター側および拠点側の認証が成功すると、IPsecの通信は自動的に確立されます(特に操作は必要ありません)。IPsec接続が完了すると、「かんたん設定ページ」のトップページに「通信中」と表示されます。

- IPsec接続をするには、センター側と拠点側で同じ認証鍵(pre-shared key)を設定する必要があります。
- 認証鍵(pre-shared key)はパスワードに相当する重要な情報です。英大文字および英小文字、数字、記号を組み合わせた分かりにくく長い値を設定して、十分に注意して管理してください。

▼

設定終了

これでIPsec通信の設定は終了です

▶IPsec接続できない場合は

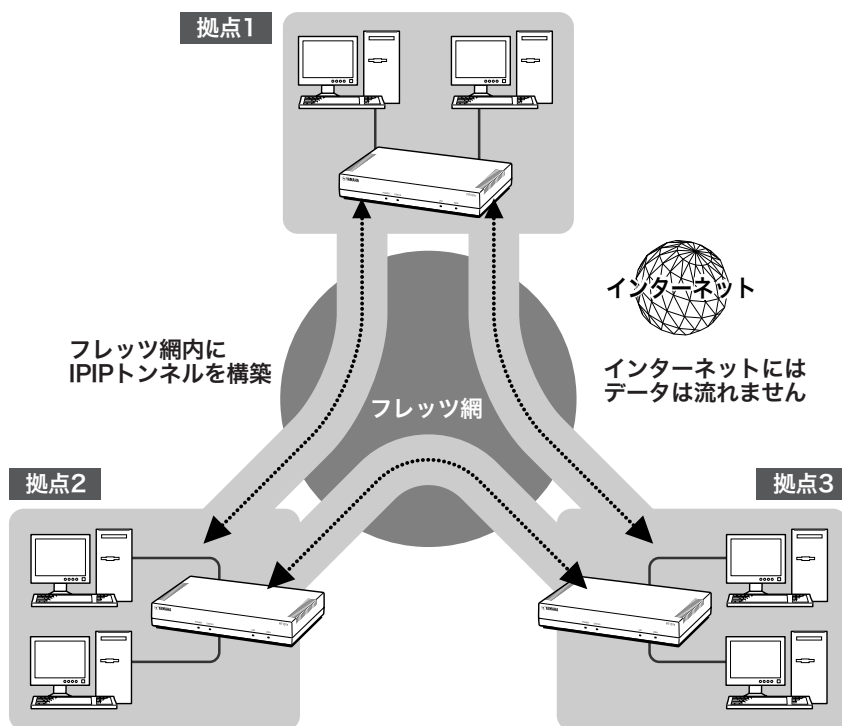
Check 1 本製品とパソコン、ADSLモデムやケーブルモデム、ONUの接続を確認してください。

Check 2 52〜53ページの設定内容をもう一度確認してください。

Check 3 それでも問題が解決しない場合は、「困ったときは」を参考にして、問題を解決してください。

接続 3

フレッツ網を使用して、LAN同士をIPIPトンネル接続する

インターネット経由でLAN同士を接続する場合は、データの盗聴や改ざんの危険性があるため、データを暗号化する必要があります。しかし、フレッツ網のように機密性の高いネットワークではデータの暗号化の必要性が低下するため、IPIPトンネルによる接続でもデータの機密を確保できます。
ここでは、NTT東日本の「フレッツ・グループアクセス ライト」やNTT西日本の「フレッツ・グループ ベーシックメニュー」のように、固定IPアドレスが1つだけ払い出される契約(端末型払い出し)でフレッツ網に接続して、IPIPトンネルでLAN同士を接続するときの設定方法を説明します。

設定する前に

- LAN同士を接続する場合には、それぞれのLANのネットワークアドレスが重複しないように、あらかじめ異なるアドレスを設定しておく必要があります。あらかじめ、本製品のLANのネットワークアドレスを変更してください。
- すでに異なるネットワークアドレスが設定されているLANに本製品を設置する場合には、設置するネットワークに合わせて本製品の設定を変更してください。詳しくは「準備5：LAN側IPアドレスを設定する」(30ページ)をご参照ください。

1. 接続方法を指定する

YAMAHA
RT107e [Rev.8.03.12 Fri Jul 1 11:56:57 2005]
ヘルプ
新しくプロバイダの設定を行ったり、修正したりします。
プロバイダ情報の設定
より詳細な設定を行ったり、本製品の通信記録を参照したりします。
詳細設定と情報
1 クリックする
詳細設定と情報
ヘルプ
下の中からやりたい項目を選び、右の設定または実行ボタンを押してください。
基本設定・VPN設定・LAN間接続の設定
基本接続の詳細な設定
設定
2 クリックする
VPN接続の設定
設定
自動接続先の設定
設定
詳細設定と情報
基本接続の詳細な設定
ヘルプ
設定可能なプロバイダ
PP[01]
設定されていません
追加
3 クリックする
PP[02]
設定されていません
追加
詳細設定と情報
プロバイダの登録
ヘルプ
PP[01]インタフェースにプロバイダの設定をします。
CATVインターネット、またはPPPoEを用いない端末型ADSL接続
PPPoEを用いる端末型ADSL接続(フレッツ・ADSL、Bフレッツ)
4 クリックする
ネットワーク型接続
CATVインターネット、またはPPPoEを用いないネットワーク型ADSL接続
PPPoEを用いるネットワーク型ADSL接続
LAN間接続
PPPoEを用いるネットワーク型 LAN間接続
次へ
5 クリックする

1. **「かんたん設定ページ」のトップページの「詳細設定と情報」をクリックする。**

   「詳細設定と情報」画面が表示されます。

2. **「基本接続の詳細な設定」の「設定」をクリックする。**

   「設定可能なプロバイダ」画面が表示されます。

3. **「追加」をクリックする。**

   「プロバイダの登録」画面が表示されます。

4. **「PPPoEを用いる端末型ADSL接続(フレッツ・ADSL、Bフレッツ)」をクリックする。**

5. **「次へ」をクリックする。**

   「プロバイダの登録/修正」画面が表示されます。

2. フレッツ網接続に必要な情報を指定する

1 「設定名」欄で、設定名を入力する。

接続先がわかるような名前を入力します。名前は自由に付けられますが、あとで設定を修正する必要が出たときなどにわかりやすい名前にしておくと便利です。

2 ユーザIDを入力する。

指定されたユーザIDを入力します。
必ず書類を確認して、間違いのないように入力してください。

3 接続パスワードを入力する。

指定されたパスワード(または自分で変更したパスワード)を入力します。
半角英数字で、大文字小文字も正確に入力してください。
入力したパスワードの文字は●で表示されます。

4 「接続先の宛先情報」欄で、接続先の宛先アドレスを指定する。

「宛先アドレス」欄

「その他」をクリックして選んでから、以下の設定を行います。

- 経路のアドレス情報:接続相手に割り当てられるIPアドレスを入力します。
- 経路のネットマスク情報:「255.255.255.255 (32ビット)」を選びます。

「宛先ドメイン名」欄

「なし」をクリックして選びます。

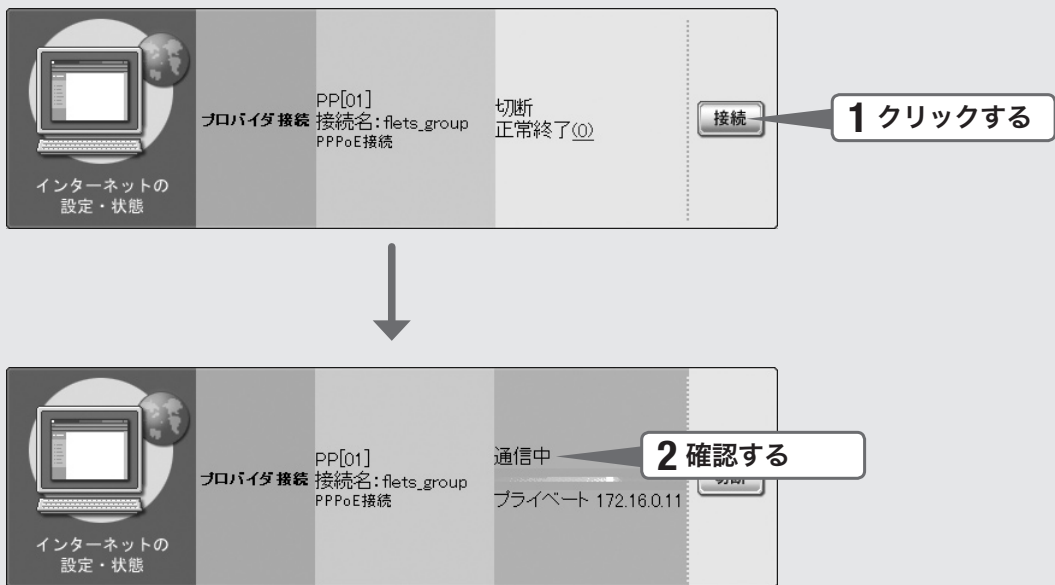
5 「設定の確定」をクリックする。

「プロバイダの登録」画面が表示されます。

6 複数のLANと接続する場合は、「戻る」をクリックしてから手順4～5を繰り返す。

接続相手に割り当てられるすべてのIPアドレスを経路に指定してください。

接続相手の宛先アドレスの設定がすべて終わったら

「トップへ戻る」をクリックして、「かんたん設定ページ」のトップページに戻ります。

3. フレッツ網に接続する

1 「接続」をクリックする。

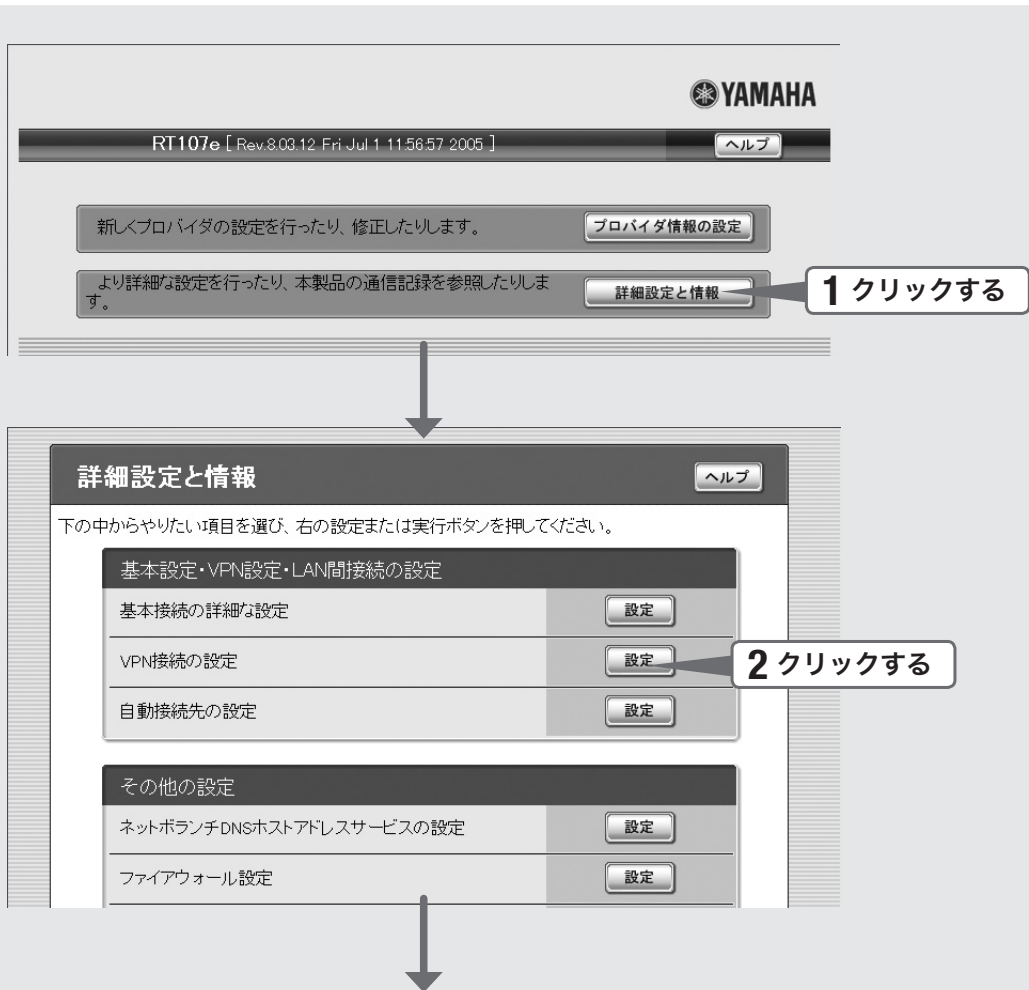
フレッツ網に接続して、「プロバイダへの接続/切断」画面が表示されます。
「トップへ戻る」をクリックすると、「かんたん設定ページ」のトップページに戻ります。

2 フレッツ網に接続しているかどうかを確認する。

画面下部の表示を見て、本製品がフレッツ網に接続していることを確認してください。
引き続き、トンネル接続の設定を行います。

フレッツ網へ接続できない場合は

- 本製品とパソコン、ADSLモデムやONUとの接続を確認してください。
- 58～59ページの設定内容をもう一度確認してください。
- それでも問題が解決しない場合は、「困ったときは」を参考にして、問題を解決してください。

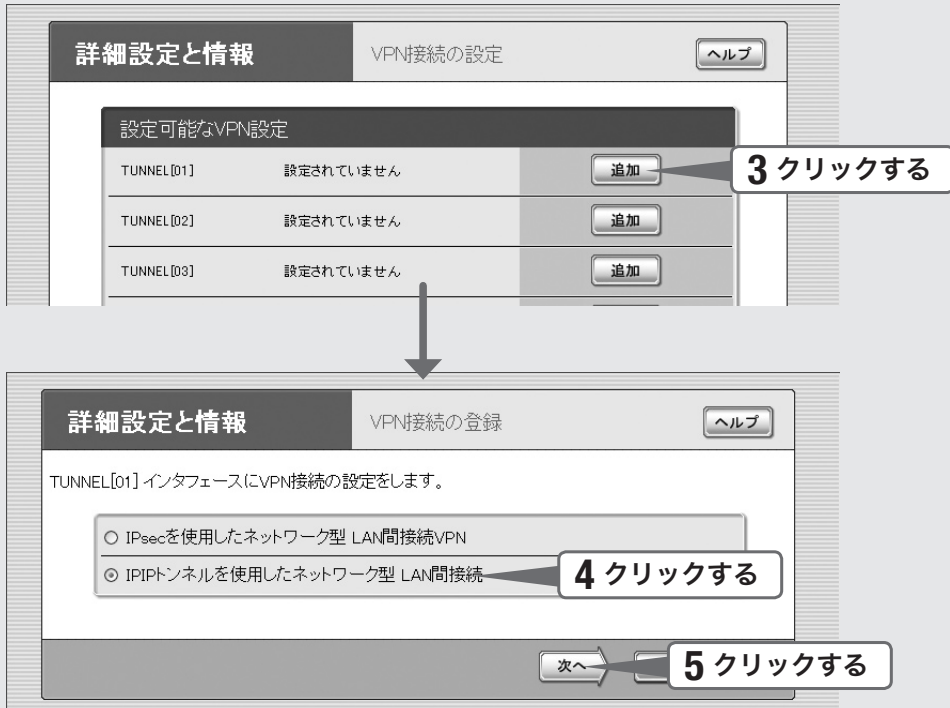
4. トンネル接続方法を選択する

1

「かんたん設定ページ」のトップページの「詳細設定と情報」をクリックする。

「詳細設定と情報」画面が表示されます。

2

「VPN接続の設定」の「設定」をクリックする。

「VPN接続の設定」画面が表示されます。

3 登録したい接続先の「追加」をクリックする。

「VPN接続の登録」画面が表示されます。

4 「IPIPトンネルを使用したネットワーク型 LAN間接続」を選ぶ。

5 「次へ」をクリックする。

「VPN接続設定の登録/修正」画面が表示されます。

5. IPIPトンネル接続に必要な情報を指定する

1 設定名を入力する。

接続先がわかるような名前を入力します。名前は自由に付けられますが、あとで設定を修正する必要が出たときなどにわかりやすい名前にしておくと便利です。

2 接続先のIPアドレスを入力する。

接続相手に割り当てられるIPアドレスを入力します。

3 接続プロバイダを指定する。

フレッツ網の接続に使用する設定(58ページで行った設定)を指定します。

ご注意

インターネット接続用のPPPoE接続を別に設定している場合は、インターネット接続用の接続設定を誤って指定しないようにご注意ください。

4

経路情報を指定する。

「経路のアドレス情報」と「経路のネットマスク情報」に、接続先のLANのネットワークアドレスを入力します。

5

「設定の確定」をクリックする。

「VPN接続設定の登録」画面が表示されます。

6

複数のLANと接続する場合は、「戻る」をクリックしてから手順4～5を繰り返す。

接続相手ごとの経路情報をすべて指定してください。

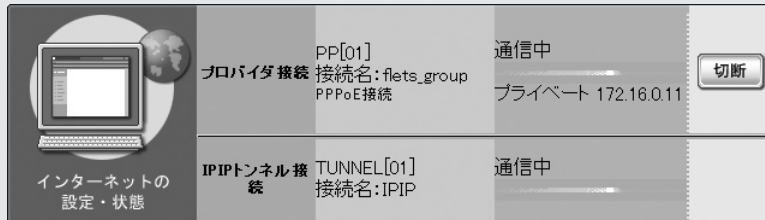
ご注意

接続相手に割り当てられるIPアドレスとその接続先のLANのネットワークアドレスの組み合わせを、間違わないように設定してください。

接続相手の経路情報の設定がすべて終わったら

「トップへ戻る」をクリックして、「かんたん設定ページ」のトップページに戻ります。

6. IPIPトンネル接続する

これまでの設定が終わると、IPIPトンネルの通信は自動的に確立されます(特に操作は必要ありません)。IPIPトンネル接続が完了すると、「かんたん設定ページ」のトップページに「通信中」と表示されます。

設定終了

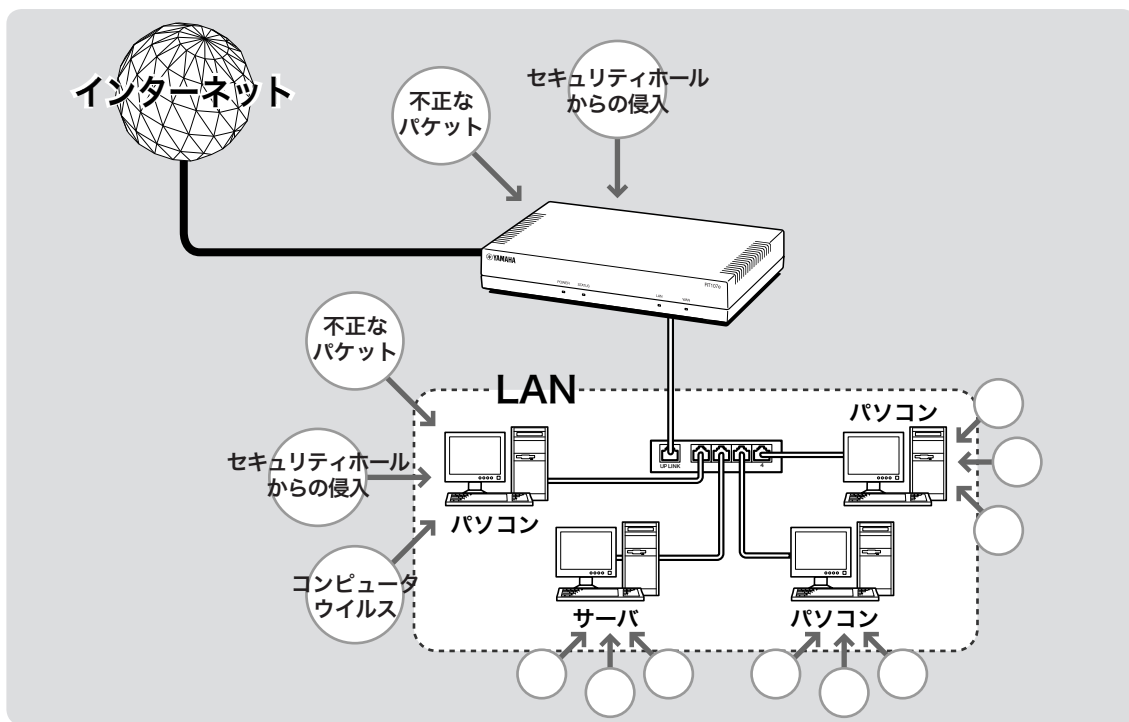
これでトンネル接続の設定は終了です

▶トンネル接続できない場合は

Check 1　本製品とパソコン、ADSLモデムやONUの接続を確認してください。

Check 2　63〜64ページの設定内容をもう一度確認してください。

Check 3　それでも問題が解決しない場合は、「困ったときは」を参考にして、問題を解決してください。

不正アクセスとセキュリティ対策の概要

インターネットからの不正アクセスとは

- インターネットに接続している間は、悪意のある者からパソコンやルーターがアタック(不正なアクセス)される可能性があります。ルーターを介してパソコンを接続している場合は、NATやIPマスカレードといったアドレス変換機能によって比較的安全ですが、設定の誤りや不足によって、同様の危険にさらされる場合があります。
- また、インターネット経由の不正アクセスだけでなく、コンピュータウイルスによる攻撃にも注意が必要です。
- 本製品の設定を改変されたり、パソコンのシステムやデータを破壊された場合、多大なデータ的被害や金銭的被害に遭うことも十分に考えられます。本製品のフィルタを設定するなどのセキュリティ対策を行って、自己防衛してください。

グローバルIPアドレスが割り当てられている場合には、特にご注意ください

悪意を持った者がアタックを行うときに主な足がかりにするのが「グローバルIPアドレス」です。同じグローバルIPアドレスを長時間使用している場合は、不正アクセスの被害にあう確率が高くなります。
固定IPアドレスサービスの利用時やネットワーク型接続、接続時に割り当てられた動的アドレスを使い続けるCATVやADSL、フレッツ・ADSLなどで接続する場合は、十分なセキュリティを設定することをおすすめいたします。

パスワード設定にもご注意ください

本製品にパスワードを設定しない状態で使用することは、セキュリティ上大変危険です。単にパスワードを設定するだけでなく、定期的にパスワードを変更するようにしてください。

不正アクセスに対抗するには

インターネットの不正アクセスは、いくつかの種類に分けられます。それぞれの種類について、以下のように対策してください。

ご注意

- 不正アクセスの手段やセキュリティ上の抜け道／穴(セキュリティホール)は、日夜新たに発見されています。本製品の機能を含めて、すべての問題を解決できる完璧なセキュリティ対策は存在せず、インターネット接続には常に危険があることをご理解ください。常に新しい情報を入手し、お客様の自己責任でセキュリティ設定を強化することを強くおすすめいたします。
- 本製品を使用した結果発生したあらゆる損失について、当社では一切その責任を負いかねますので、あらかじめご了承ください。

1. 不正なパケットで侵入するもの

- インターネットへの接続の切断や、グローバルIPアドレスの変更がもっとも効果的です。
- パケットフィルタリング式ファイアウォールで、不要なパケットを通さないことも、ある程度効果があります。
- アプリケーション・ゲートウェイ式ファイアウォールソフトウェアも、整合性のないパケットや不審なActiveX、Javaアプレットをパソコンに受け入れないようにするため、かなり効果があります。ウィルス検知ソフトと組み合わせて使うこともできます。ただしこの場合は、ファイアウォール用サーバを設けて、アプリケーション・ゲートウェイ式ファイアウォールソフトウェアをインストールする必要があります。

本製品で可能な対策

- 自動切断機能を設定することで、接続/切断のたびに動的IPアドレスを変更できます。ただし、サーバ公開用途に本製品を使用する場合には、この対策を実施することは困難となりますので、サーバ側で対策を行ってください。
- 攻撃に使用される特定の種類のパケットを通さないようにフィルタを設定する(70ページ)ことで、その攻撃を防御できることがあります。

2. OSやサーバソフトウェアのセキュリティホールから侵入するもの

OSやサーバソフトウェアのバージョンアップや、適切な設定／運用を行うことで、かなり防止できます。

本製品で可能な対策

- 本製品の設定を変更できるホストを制限して、悪意のある第三者が本製品の設定を勝手に変更することを防止できます(74ページ)。
- 攻撃に使用される特定の種類のパケットを通さないようにフィルタを設定する(70ページ)ことで、その攻撃を防御できることがあります。

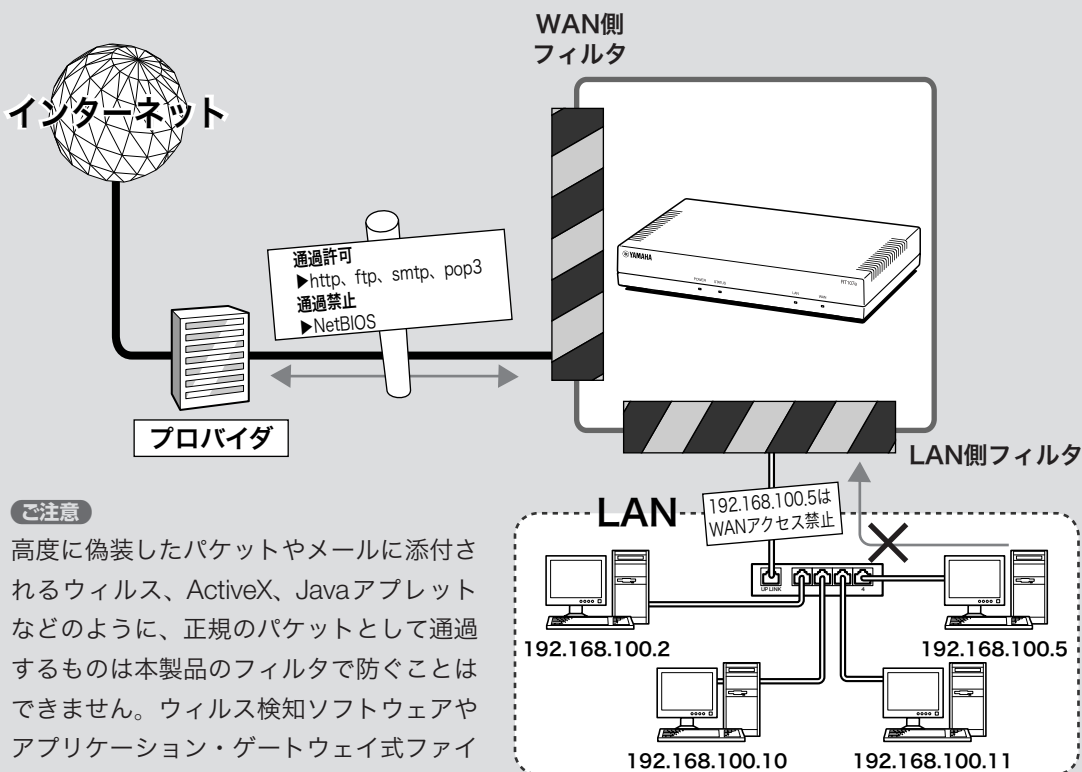
3. 電子メールの添付ファイルとして侵入するもの(コンピュータウイルス)

添付ファイルを開くことで感染します。不審な添付ファイルは開かないことを徹底するだけでなく、パソコンにウィルス検知ソフトウェアをインストールして、ウィルスを早期発見／早期駆除することで、被害を最小限に抑えることができます。

本製品で可能な対策

- 本製品のセキュリティ強化機能は、コンピュータウイルスには効果がありません。
- パソコン用のウィルス検知ソフトウェアを別途ご用意ください。

フィルタを設定する

本製品では、接続先ごとに100個までのフィルタを設定できます。それぞれのフィルタでパケットの送信元や送信先、パケットの種類、プロトコルの種類、方向によって、パケットを通さないよう設定できます。不正なアクセスに使われやすいパケットやあり得ないパケットをルーター通過時に破棄するように設定することで、不正なパケットがLAN内に入ることを防ぐことができます。

ご注意

高度に偽装したパケットやメールに添付されるウィルス、ActiveX、Javaアプレットなどのように、正規のパケットとして通過するものは本製品のフィルタで防ぐことはできません。ウィルス検知ソフトウェアやアプリケーション・ゲートウェイ式ファイアウォールソフトウェアを併用するようおすすめいたします。

「パケット」とは？

ネットワークを流れるデータの単位です。
ネットワークに流れているデータはパケット単位で分割され、それぞれが発信元や送信先、データの種類などの情報を持っています。
フィルタを設定することで、パケットの条件を設定して不要な自動接続を防止したり、パケットの行き先を指定して複数の接続先を使い分けたりすることができます。

本製品のフィルタの特徴

静的フィルタと動的フィルタ

本製品で設定できるフィルタには、次の2種類があります。実際に使用する場合は、それぞれの良いところを併用しながら設定を行います。

- **静的フィルタ：**一度設定を行うと、データや通信の有無にかかわらず常に有効になります。
- **動的フィルタ：**通信状態を監視しながら、必要に応じてフィルタが有効になります。例えば「通常はインターネットからLANへのデータはすべて禁止にしておき、LAN側からftpのアクセスが発生したときだけ許可する」といった設定ができます。

「かんたん設定ページ」で接続先を登録すると、基本的なフィルタが適用されます

「かんたん設定ページ」で接続先を登録するだけで、接続の種類に応じて自動的に以下のフィルタが自動的に適用されます。この基本的なフィルタに加えて、必要に応じてフィルタを追加して登録・適用できます。

ご注意
- セキュリティレベルや設定内容は予告なく変更する場合があります。
- コンソールで接続先を設定した場合は、フィルタは何も登録されていない状態になります。

プロバイダ接続の場合

フィルタの組み合わせパターンで、7段階のセキュリティレベルを定義しています。プロバイダの新規登録時にはセキュリティレベル6の設定を自動的に適用します。セキュリティレベルは、必要に応じて後で変更することができます(次ページ)。

フィルタ番号の意味

本製品のフィルタ機能の番号は、ほぼ無制限に利用できますが、「かんたん設定ページ」では各接続先毎に100個(0番〜99番)ずつ設定できるようになっています。以下に「かんたん設定ページ」の利用する、フィルタ番号の対応を示します。

割当領域	コンソールコマンドのフィルタ番号
LAN/WANポート用領域	100000〜199999
接続先設定用領域(PP01~)	200000〜299999
フィルタ型ルーティング用領域	500000〜599999

ご注意
- セキュリティのために、フィルタの設定変更は機能を十分にご理解の上、行ってください。
- フィルタを多く適用すると処理が複雑になり、インターネットへのアクセス速度が遅くなる場合があります。

フィルタを登録する

セキュリティを目的としたフィルタ設定の考えかた

フィルタを設定するときは、以下の考えかたを基本にすることをおすすめします。

LAN側からインターネット側へのアクセス（出力方向）は原則許可し、必要に応じて禁止する

LAN側からインターネット側へのアクセスを厳しく規制すると非常に使いにくいものになり、管理や設定変更に手間がかかります。原則自由とした上で、問題があればその部分だけ制限します。

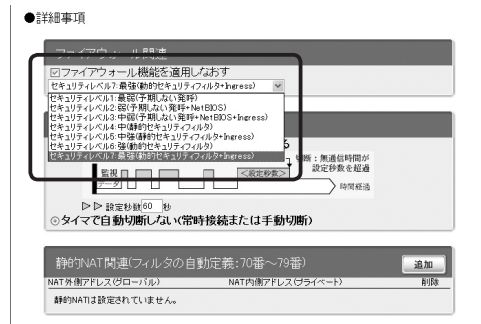
インターネット側からLAN側へのアクセス（入力方向）は、原則禁止し、必要に応じて許可する

インターネット側からLAN側へのアクセスは、原則禁止して外部からのアクセスを防ぎます。Webサーバの公開など、必要がある場合にのみ最小限だけ許可します。

ご注意

インターネット側からのアクセスとは、インターネット側からリクエストが始まったパケットのことを指します。LAN側からリクエストしたパケットの応答パケットにはACKフラグという識別子が付くので、インターネット側からのアクセスとは区別して、フィルタで通過させることができます。

初期設定のフィルタセットを選ぶ（セキュリティレベル）

本製品の「かんたん設定ページ」では、フィルタを組み合わせた7段階のセキュリティレベルが定義されています。プロバイダの新規登録時に、接続の種類にあわせて自動的にセキュリティレベルが設定されます（前ページ）。設定されたセキュリティレベルは、「プロバイダの登録／修正」画面であとから変更することもできます。

設定内容について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

「プロバイダの登録／修正」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」

▶「基本接続の詳細な設定」の「設定」

▶設定を変更したい接続先の「設定」

「かんたん設定ページ」で手動でフィルタを作成する

フィルタを設定するには、「ファイアウォールの設定」画面を使用します。

ご注意

- LANを選ぶと、LANポートに接続しているパソコン、およびLANポートに接続しているHUBに接続しているすべてのパソコンが対象になります。
- フィルタの具体的な設定例については、「コマンドリファレンス」(付属CD-ROMに収録)をご覧ください。

設定内容について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

「ファイアウォールの設定」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」
▶「ファイアウォール設定」の「設定」
▶ファイアウォールを設定したいインタフェースの「設定」(IPv6で接続している場合は、「IPv6フィルタ」の「設定」をクリックします)

フィルタのコマンドを直接入力して、フィルタを作成する

フィルタのコマンドを直接入力して、フィルタを作成することもできます。あらかじめテキストエディタなどでフィルタのコマンドを作成しておき、複数のルーターにフィルタを適用したいときなどに便利です。

フィルタのコマンドを直接入力するには、「かんたん設定ページ」の「コマンドの実行」画面を使用します。

ヒント

フィルタのより専門的な設定例や文法については、「コマンドリファレンス」(付属CD-ROMに収録)やヤマハルーターホームページ(http://NetVolante.jp/、http://www.rtpro.yamaha.co.jp/)をご覧ください。

「コマンドの実行」画面を開くには

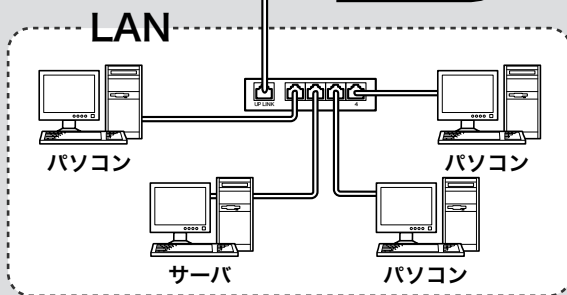
「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」
▶「コマンドの実行」の「実行」

不正アクセスを検出して警告する

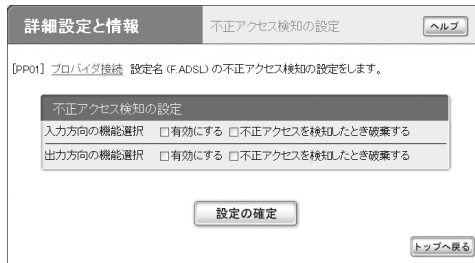
不正アクセス検知機能はインターネットからの侵入や攻撃などを検出して、警告する機能です。
検知情報を元に不審な発信元やアプリケーションを通さないフィルタを設定することで、
よりセキュリティを高めることができます。

ご注意

- 不正アクセスの手段や侵入／攻撃パターンは日夜新たに発見されており、それを防ぐ完璧な手段はありません。この機能ですべての不正アクセスを検知できるものではありませんので、あらかじめご了承ください。
- この機能は侵入／攻撃パターンに近いものを検知する機能ですので、タイミングなどさまざまな理由により、検知できない場合があります。また、検知されたパターンが必ずしも重大な不正アクセスであることを判断するものではありません。あくまでセキュリティ管理の目安であることをご理解の上、ご利用ください。
- 本機能は各インタフェースおよび入出力に適用できます。
- 本機能を使用すると、インターネットなどへのアクセス速度が遅くなります。

不正アクセス検知機能を設定する

「不正アクセス検知の設定」画面で、PP（プロバイダなどの外部接続側）やLAN（LAN接続側）のインタフェースごとに、検知するパケットの方向や検知時の処理方法を設定できます。

ご注意

不正アクセス検知機能は各インタフェースおよび入出力に適用可能ですが、適用数によってはインターネットなどへのアクセス速度が遅くなります。

設定内容について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

「不正アクセス検知の設定」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」
▶「ファイアウォール設定」の「設定」
▶不正アクセス検知機能の設定を変更したいインタフェースの「不正アクセス検知」の「設定」

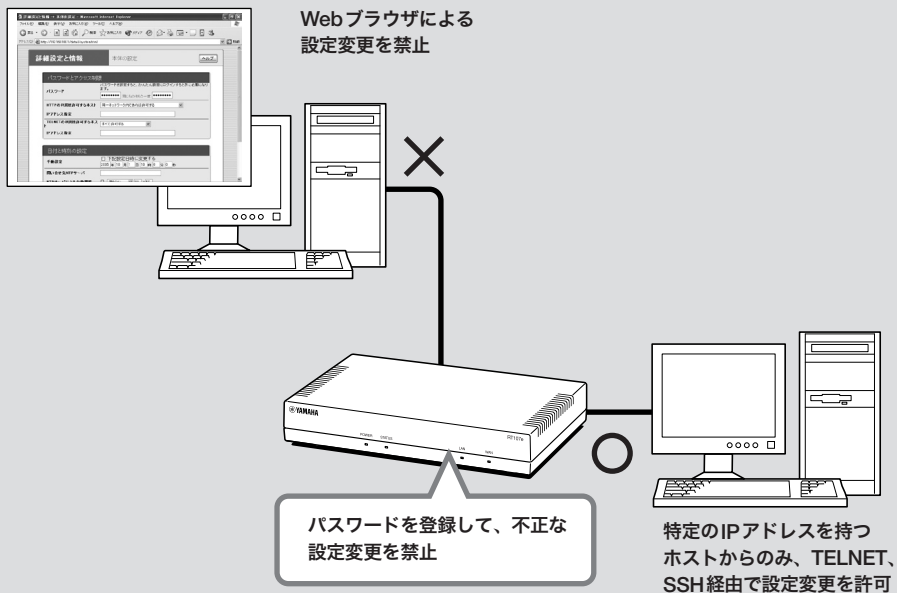
不正アクセス検知履歴を確認する

不正アクセス検知履歴を確認します。
「かんたん設定ページ」のトップページ－「詳細設定と情報」－「システム情報のレポート作成」画面の「不正アクセス検知情報」欄で、不正アクセス検知の履歴を確認できます。

ご注意

- 「システム情報のレポート作成」画面の「不正アクセス検知情報」欄は、不正アクセス検知を有効にしてないと表示されません。
- 不正アクセスの手段や侵入／攻撃パターンは日夜新たに発見されており、それを防ぐ完璧な手段はありません。この機能ですべての不正アクセスを検知できるものではありませんので、あらかじめご了承ください。
- この機能は侵入／攻撃パターンに近いものを検知する機能ですので、タイミングなどさまざまな理由により、検知できない場合があります。また、パターンが検知された場合でも、それが重大な不正アクセスであるとは限りません。あくまでセキュリティ管理の目安であることをご理解の上、ご利用ください。

本製品の設定を変更できるホストを制限する

本製品には、本製品自体のセキュリティを確保するために、パスワード機能や利用ホスト制限機能を装備しています。これらの機能を利用することで、第三者が不正にルーターの設定を変更できないように設定できます。

「ユーザとアクセス制限の設定」画面で、Webブラウザ(HTTP)やTELNET、SSHソフトウェアを使って本製品の設定を変更できるホストを制限できます。指定したIPアドレスのホストのみ本製品にアクセスできるように設定することもできます。

設定内容について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

「ユーザとアクセス制限の設定」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」

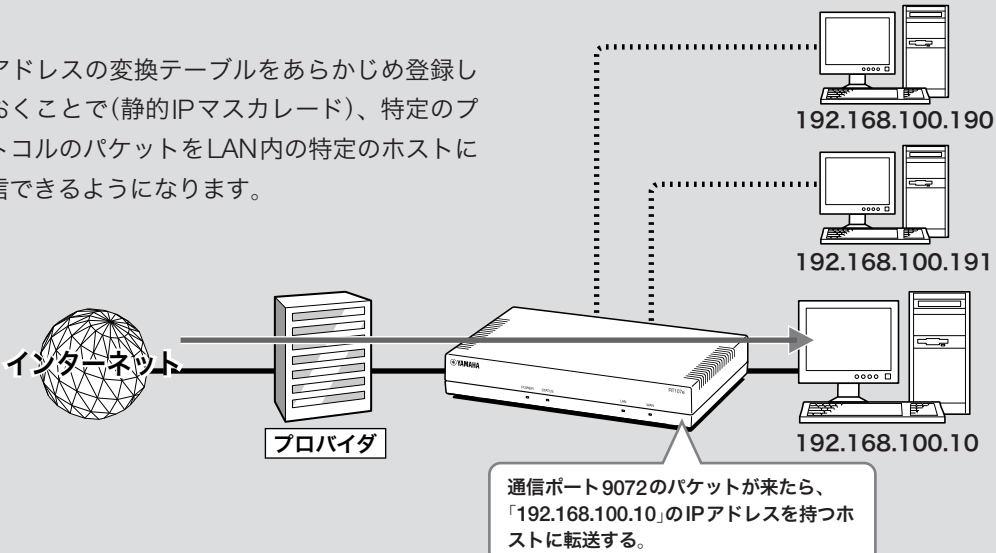
▶「ユーザとアクセス制限の設定(HTTP、TELNET、SSH)」の「設定」

グローバルIPアドレスが必要なサービスをLAN内から利用する

グローバルIPアドレスが必要なアプリケーションソフトウェアをルーターのLAN側から利用しようとしても、正しく動作しない場合があります。以下の順序で問題を解決してください。

1. プロトコルとポート番号、ホストのIPアドレスの変換テーブルを登録する(静的IPマスカレード)。
2. DMZホスト機能を利用する。

1. 静的IPマスカレード設定で問題を解決する

IPアドレスの変換テーブルをあらかじめ登録しておくことで(静的IPマスカレード)、特定のプロトコルのパケットをLAN内の特定のホストに送信できるようになります。

1. パソコンのIPアドレスを設定する

外部からのアクセスを許可するパソコンに、固定プライベートIPアドレスを設定します。

2. IPアドレスの変換テーブルを登録する

「静的IPマスカレードの登録」画面で、通信プロトコルとポート番号、ホストのIPアドレスの変換テーブルを登録します(静的IPマスカレード設定)。

ご注意

- プロトコルやポート番号については、利用するソフトウェアやサービスの説明書をご覧ください。
- 代表的なソフトウェアについては、「静的IPマスカレードの登録」画面で「ヘルプ」をクリックすると、使用するポート番号などの設定例を確認できます。

設定内容について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

「静的IPマスカレードの登録」画面を開くには

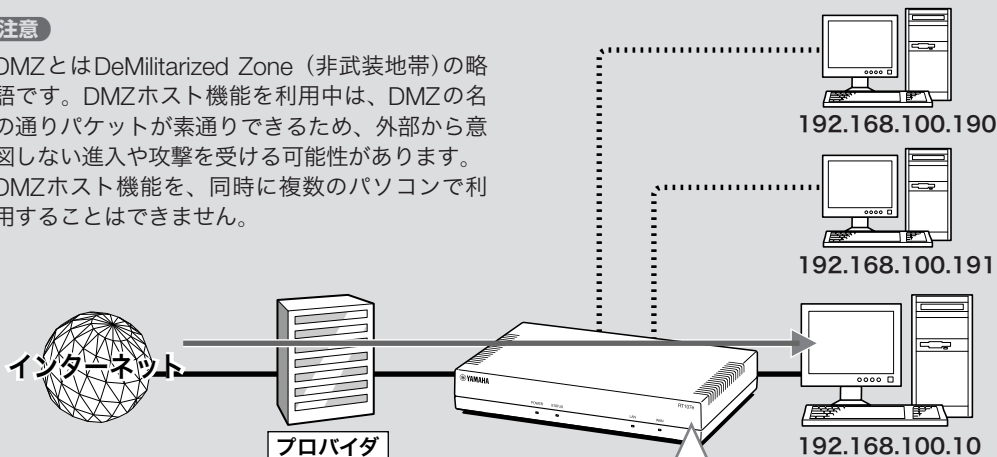
「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」
▶「基本接続の詳細な設定」の「設定」
▶設定を変更したい接続先の「設定」
▶「静的IPマスカレード関連」欄の「追加」

2. DMZホスト機能を使って問題を解決する

本製品がNAT/IPマスカレードテーブルに登録されていない宛先へのパケットを受信したときに、特定のIPアドレスのホストに転送するように設定できます(DMZホスト機能)。

ご注意

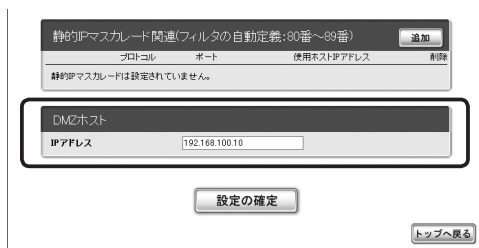
- DMZとはDeMilitarized Zone（非武装地帯)の略語です。DMZホスト機能を利用中は、DMZの名の通りパケットが素通りできるため、外部から意図しない進入や攻撃を受ける可能性があります。
- DMZホスト機能を、同時に複数のパソコンで利用することはできません。

ヒント

内部アドレスと分離することで、公開サーバなどが攻撃を受けても、内側アドレスのホストへの被害を防ぐことができます。

1. パソコンのIPアドレスを設定する

外部からのアクセスを許可するパソコンに、固定プライベートIPアドレスを設定します。

2. DMZホストのアドレスを指定する

「プロバイダの登録／修正」画面で、DMZホストのアドレスを設定します。

設定内容について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

「プロバイダの登録／修正」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」

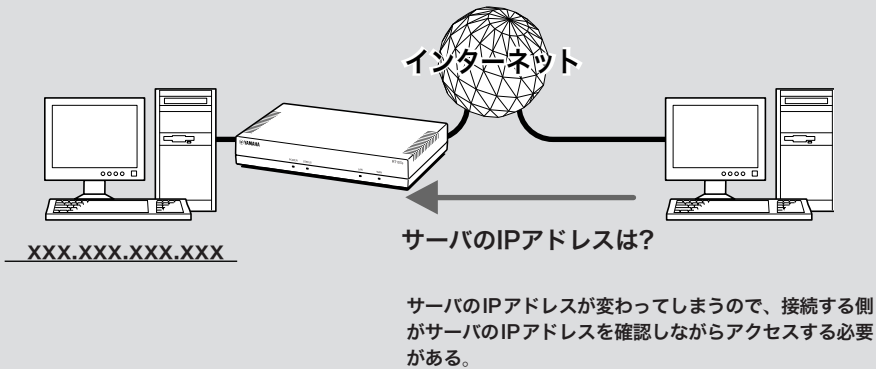
▶「基本接続の詳細な設定」の「設定」

▶設定を変更したい接続先の「設定」

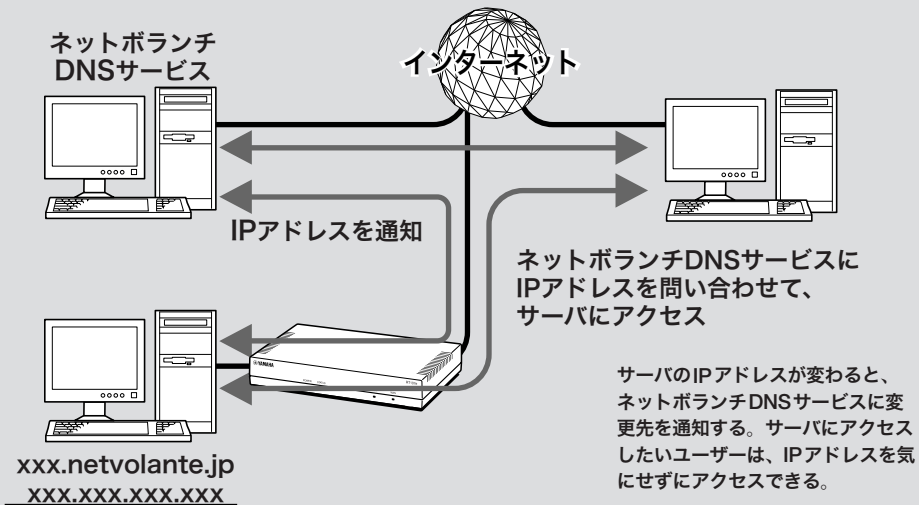
ネットボランチDNSサービスを利用する

ネットボランチDNSサービスとは?

サーバを構築してホームページを公開したり、作業用のファイルをインターネット経由で共有したりするためには、相手のグローバルIPアドレスがわかっている必要があります。
しかし、インターネットに常時接続している場合でも、割り当てられるグローバルIPアドレスは再接続時または時間によって変更される場合があります。そのため、グローバルIPアドレスが固定で割り当てられない接続サービスを利用していると、サーバを構築して公開することは困難でした。

サーバのIPアドレスが変わってしまうので、接続する側がサーバのIPアドレスを確認しながらアクセスする必要がある。

ネットボランチDNSサービスを利用すると

グローバルIPアドレスが変更されるごとにIPアドレスがサーバへ通知されるため、固定のホスト名を持つことができるようになります。したがって、固定IPアドレスサービスを契約していなくても自宅サーバで独自ドメインを使った各種サーバを運用したり、IPsecを利用してVPNを構築して、外部とデータをやり取りしたりできるようになります。

サーバのIPアドレスが変わると、ネットボランチDNSサービスに変更先を通知する。サーバにアクセスしたいユーザーは、IPアドレスを気にせずにアクセスできる。

ネットボランチDNSサービスで取得できるホスト名

ネットボランチDNSサービスを利用すると、「(ユーザの希望ホスト名).xxx.netvolante.jp」という形式のホスト名を取得できます。「xxx」の部分は、ネットボランチDNSサーバが任意に自動で割り当てます。グローバルIPアドレスが変更されるごとに設定を変更する必要がなくなり、便利です。

ご注意

- ネットボランチDNSサービスは、端末型プロバイダ接続に対してのみ設定できます。ネットワーク型接続やLAN間接続には設定できません。なお、端末型CATVプロバイダ接続の設定でも、WAN側IPアドレスが固定アドレスの場合は設定できません。
- ホストアドレスはルーター1台につき1つしか取得できません。
- 希望のホスト名が取得できるとは限りません。あらかじめご了承ください。
- 取得したホストアドレスに関しての正引きはできますが、逆引きはできません。
- ネットボランチDNSサービスはヤマハ独自のプロトコルを使用しているため、取得したホストアドレスを外部のダイナミックDNSサーバに登録することはできません。
- ネットボランチDNSサービスは、プロバイダからグローバルIPアドレスが割り当てられている環境でのみ利用できます。グローバルIPアドレスとは、下記以外のIPアドレスです。
  - 10.0.0.0〜10.255.255.255
  - 172.16.0.0〜172.31.255.255
  - 192.168.0.0〜192.168.255.255
- ご利用中のプロバイダによっては、ホスト名の登録／更新内容がネットボランチDNSサービスにすぐに反映されないことがあります。あらかじめご了承ください。

ネットボランチDNSサービスでホストアドレスを取得する

ネットボランチDNSサービスを利用するには、「ネットボランチDNSホストアドレスサービスの設定」画面を使用します。

ご注意

- ホストアドレスはルーター1台につき1つしか取得できません。
- ホストアドレスサービスを設定するときは、希望のホスト名のみを「ホスト名」欄に入力してください。

設定内容について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

「ネットボランチDNSホストアドレスサービスの設定」画面を開くには

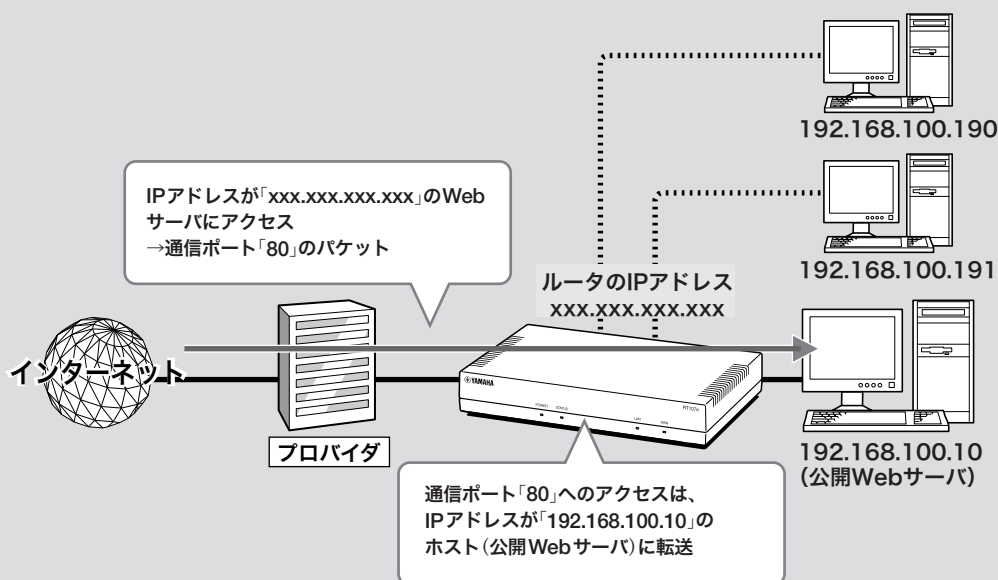
「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」
▶「ネットボランチDNSホストアドレスサービスの設定」の「設定」

ホストアドレスを取得できない場合は

- 契約プロバイダによっては、登録／更新してすぐに名前解決ができない場合があります。しばらく時間をおいてから再度試してみてください。
- プロバイダからグローバルIPアドレスが割り当てられているかどうかを確認してください。
- プロバイダの設定で指定したDNSサーバのIPアドレスが正しいかどうかを確認してください。

外部にサーバを公開する

インターネットへサーバを公開したい場合は、公開したいサーバに固定プライベートIPアドレスを設定してから、IPアドレスの変換テーブルを登録します（静的IPマスカレード）。このあとに本製品にLAN外からのアクセスを許可するフィルタを設定すれば、特定のプロトコルのパケットをLAN内のサーバに送信できるようになるため、インターネットからサーバにアクセスできるようになります。

ご注意

LANの外部にサーバを公開するときは、データを保全するために十分なセキュリティ設定を行ってください。セキュリティ設定が不十分の場合は、双方のLANに接続されたパソコンが不正侵入や盗聴、妨害、データの消失、破壊などにあう可能性があります。

ヒント

ネットボランチDNSサービスを利用することで、固定グローバルIPアドレスが割り当てられない接続サービスでも、サーバを公開して運用できます。詳しくは「ネットボランチDNSサービスを利用する」（78ページ）をご覧ください。

設定の流れ

サーバを公開するためには、次の設定が必要です。

ルーターの設定

- プロトコルとポート番号、サーバのIPアドレスの変換テーブルを登録する（静的IPマスカレード、次ページ）。
- アクセスを許可する設定に変更する（次ページ）。

サーバの設定

- パソコンのIPアドレスを設定する。
- WebやFTPなど、公開するサービスに合わせてファイルサーバソフトの設定を変更する。

IPアドレスの変換テーブルを登録する

「静的IPマスカレードの登録」画面で、通信プロトコルとポート番号、サーバのIPアドレスの変換テーブルを登録します(静的IPマスカレード設定)。

ご注意

- プロトコルやポート番号については、利用するソフトウェアやサービスの説明書をご覧ください。
- 代表的なソフトウェアについては、「静的IPマスカレードの登録」画面で「ヘルプ」をクリックすると、使用するポート番号などの設定例を確認できます。

設定内容について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

「静的IPマスカレードの登録」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」

▶「基本接続の詳細な設定」の「設定」

▶設定を変更したい接続先の「設定」

▶「静的IPマスカレード関連」欄の「追加」

アクセスを許可する設定に変更する

サーバに対するアクセスを許可するため、サーバのIPアドレスや通信プロトコルを指定したフィルタを設定します。この場合、LAN内のその他のパソコンに外部からアクセスすることはできません。フィルタを設定するには、「ファイアウォールの設定」画面を使用します。

ご注意

- 公開する相手を限定したい場合は、「送信元IPアドレス」欄に相手のIPアドレスを指定します。
- 「受信先ポート番号」は、利用したいサーバアプリケーションの使用プロトコルに設定してください。
- 使用できるフィルタ番号は、各接続先毎に0～99の100個です。フィルタやプロトコルなどについて詳しくは、「コマンドリファレンス」(付属CD-ROMに収録)をご覧ください。

(Webサーバを公開する場合の入力例)

設定内容について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

「IPフィルタの登録」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」

▶「ファイアウォール設定」の「設定」

▶ファイアウォールを設定したいインタフェースの「設定」(IPv6で接続している場合以外は、「IPv4フィルタ」の「設定」をクリックします)

▶「IPv4静的IPフィルタの一覧」画面の「追加」

IPv6環境で使う

本製品は次世代インターネット・プロトコルである「IPv6」(Internet Protocol Version 6)をサポートしています。従来の「IPv4」に関する機能も継承しているため、既存のネットワークに影響を与えずに、IPv6を利用できます。

ご注意

プロバイダがIPv6に対応していない場合、IPv6環境でインターネットに接続できません。契約しているプロバイダがIPv6接続サービスを提供しているかどうか、あらかじめご確認ください。

IPv6を導入する前に

IPv6とIPv4環境を混在させる場合は

IPv6はIPv4との互換性がないため、両者をネットワーク上で混在させる場合は、移行技術(Transition Mechanism)と総称される仕組みが必要です。また、一般的にはIPv4からIPv6への移行は複数の段階を踏むことになるため、それぞれの段階に応じた移行技術が必要になります。
本製品では、IPv4ネットワークを経由してIPv6ネットワークを接続するための「IPv6 over IPv4トンネリング」、IPv6ネットワークを経由してIPv4ネットワークを接続するための「IPv4 over IPv6トンネリング」を移行技術としてサポートしています。

プロバイダからの設定情報を確認する

IPv6接続サービスを契約すると、以下の情報がプロバイダから提供されます。

- プレフィックス(アドレスブロック)
- 接続方法(ネイティブ接続／デュアルスタック接続／トンネル接続)
- トンネルの終端アドレス(トンネル接続の場合)
- 経路制御方法(RIPngを使うか使わないか。特に記載がない場合、RIPngは使用しません。)
- 接続の確認方法(ping6の相手アドレスや、閲覧するWebサイトなど)

Windows XPでIPv6を導入する

コマンド プロンプトで、以下のコマンドを入力します。

```
ipv6 install
```

ヒント

IPv6環境の導入について詳しくは、「スタート」–「ヘルプとサポート」をクリックして表示される、Windows XPのヘルプをご覧ください。「検索」欄に「IPv6」と入力すると、関連する情報が表示されます。

IPv6を使えるように設定する

設定を始める前に、「IPv6の設定」画面でIPv6で接続する相手（プロバイダ）を登録します。

ご注意

プロバイダを登録していない場合は、IPv6接続の操作を行ってもエラーが発生します。

設定内容について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

「IPv6の設定」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」

▶「IPv6の設定」の「設定」

IPv6接続を確認する

以下の手順で、IPv6環境が正しく設定されているかどうか確認します。

ヒント

本製品とパソコンは、LANケーブルで接続した時点で通信可能になります。パソコン側での設定は、特に必要ありません。

1 LAN側の接続を確認する。

LANポートに接続されたパソコンから、本製品のLAN1アドレスにping6を実行します。

返事があれば、正しく設定されています。

ヒント

本製品のLAN1アドレスは、プレフィックスに「1」をつけたアドレスになります。
例：プレフィックスが「fec0:12ab::/64」の場合

- LAN1アドレスは「fec0:12ab::1/64」になります。
- 本製品のLAN1アドレスにping6を実行するには、「ping6 fec0:12ab::1」とコンソールで入力してから、Enterキーを押します。

2 LAN側とWAN側の接続を確認する。

プロバイダへping6を実行したり、専用のWebサイトを閲覧するなど、プロバイダから指定されている確認手順を行います。
これでIPv6環境が利用できるようになりました。

UPnP機能の動作設定を変更する

UPnP機能とは？

UPnPとはUniversal Plug and Playの略で、ネットワーク上でUPnP対応OSがUPnP対応機器を自動的に検出して、相互接続しやすくするための仕組みのことです。本製品はUPnPをサポートしているため、本製品を設置したLAN内にあるWindows XPを搭載しているパソコンからWindows Messengerの音声チャットなどを利用できます。

ご注意

- 本製品のUPnP機能は、UPnP Forumで規定されている機能すべてに対応しているわけではありません。
- CATV接続など、プロバイダから割り当てられるIPアドレスがプライベートIPアドレスの場合は、UPnP機能を使用したWindows Messengerによる音声チャットは使用できません。
- 「かんたん設定ページ」でUPnP機能の設定を行うには、あらかじめ接続プロバイダを登録しておく必要があります。
- プロバイダを登録せずにWindows MessengerなどのUPnP環境を必要とするソフトウェアを起動すると、ルーターとの通信に時間がかかるようになります。この場合は、接続プロバイダを登録するか、UPnP機能を停止してください。
- Windows Messengerの終了／起動を繰り返したり、ルーターの再起動や回線の切断などによってパソコンとルーターでUPnP機能の情報が異なると、正常に接続できなくなることがあります。
  この場合は、回線を接続した状態でいったんWindows Messengerをサインアウトしてから、Windows Messengerを再起動します。それでも接続できない場合は、パソコンを再起動してください。

パソコン側でUPnP機能を使えるか確認する

以下の手順で、お使いのパソコンがUPnP機能を使える状態かどうか確認してください。

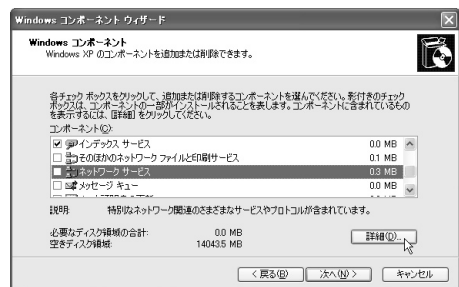
ヒント

UPnP環境の導入について詳しくは、「スタート」–「ヘルプとサポート」をクリックして表示される、WindowsXPのヘルプをご覧ください。「検索」欄に「UPnP」と入力すると、関連する情報が表示されます。

1 「スタート」ボタンをクリックして、「コントロール パネル」をクリックする。

2 「プログラムの追加と削除」をクリックする。

3 画面左側の「Windowsコンポーネントの追加と削除」をクリックする。

4 「ネットワーク サービス」をクリックして選んでから、「詳細」をクリックする。

5 「ユニバーサル プラグ アンド プレイ」にチェックが付いているかどうか確認する。

- チェックが付いていれば、パソコン側でUPnP機能が利用できるようになっています。
- チェックが付いていない場合は、引き続き手順6以降の操作を行います。

6 「ユニバーサル プラグ アンド プレイ」にチェックを付けてから、「OK」をクリックする。

7 「次へ」をクリックする。

以後は画面の指示に従って、インストールを行ってください。

UPnPを使えるように設定する

本製品のUPnP機能は工場出荷状態では「使用しない」になっています。本製品のUPnP機能を使用するためには、「UPnPの設定」画面で設定を「使用する」に変更してください。

設定内容について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

「UPnPの設定」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」

▶「UPnPの設定」の「設定」

フレッツ・スクウェアを利用する

フレッツ・ADSLやBフレッツでインターネットに接続している場合は、NTT東日本またはNTT西日本が運営するフレッツ・スクウェアに接続して、様々なコンテンツを楽しめます。
通常の接続先（フレッツ・ADSLまたはBフレッツ）に接続している状態で、フレッツ・スクウェアにも接続するには、以下の手順で操作します。

ご注意

- フレッツ・ADSLまたはBフレッツを契約していない場合は、以下の操作を行ってもフレッツ・スクウェアには接続できません。
- NTT東日本と契約している場合は、接続先の宛先情報を追加で設定する必要があります。詳しくは、http://NetVolante.jp/ の情報を参照してください。

1 **PPPoEを用いる端末型ADSL接続（フレッツ・ADSL、Bフレッツ）用の「プロバイダの登録/修正」画面で、必要な設定項目を入力する。**

NTT東日本とフレッツ接続サービス（フレッツ・ADSLまたはBフレッツ）を契約している場合は

- **ユーザID：**「guest@flets」と入力します。
- **パスワード：**「guest」と入力します。

NTT西日本とフレッツ接続サービス（フレッツ・ADSLまたはBフレッツ）を契約している場合は

- **ユーザID：**「flets@flets」と入力します。
- **パスワード：**「flets」と入力します

NTT東日本とフレッツ接続サービスを契約している場合の入力例

接続先の宛先情報

- **宛先アドレス：**「プライベートアドレスのネットワーク」を選びます。
- **宛先ドメイン名：**「指定する」を選んでから、「flets」と入力します。

ファイアウォール関連

「セキュリティレベル6：強（動的セキュリティフィルタ）」を選びます。

設定内容について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

PPPoEを用いる端末型ADSL接続（フレッツ・ADSL、Bフレッツ）用の「プロバイダの登録／修正」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

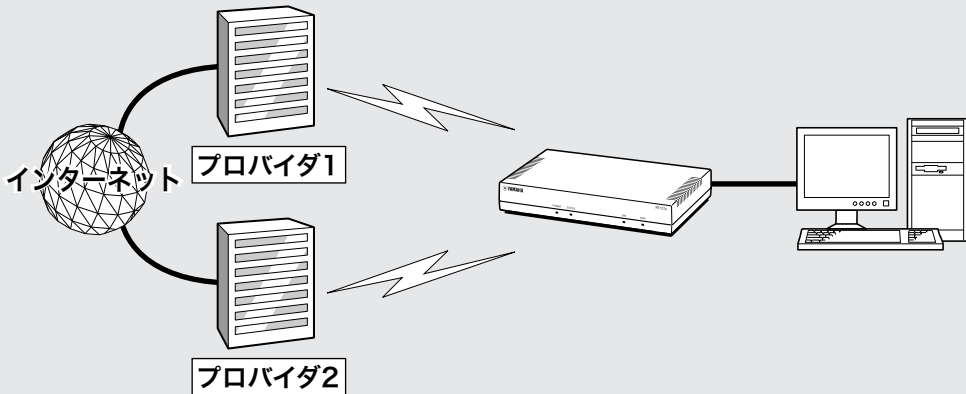
▶トップページの「詳細設定と情報」
▶「基本接続の詳細な設定」の「設定」
▶設定を追加したい接続先の「追加」
▶「PPPoEを用いる端末型ADSL接続（フレッツ・ADSL、Bフレッツ）」を選んでから、「次へ」

2 **「設定の確定」をクリックする。**

これまでの設定内容が、入力した「設定名」として保存されます。

3 **Webブラウザのアドレスバーに「http://www.flets/」と入力して、フレッツスクウェアに接続できることを確認する。**

複数の接続先を使い分ける

通常使用する接続先ともう1つ別の接続先を登録しておき、通常使用する接続先がメンテナンスなどのために接続できない場合に、もう1つの接続先に手動で接続するという使いかたができます。

自動接続先を使い分ける

「自動接続先の設定」画面で、自動接続先または「接続」をクリックして手動接続を行う場合に接続先を切り替えるかどうかを設定します。

設定内容について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

「自動接続先の設定」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」

▶「自動接続先の設定」の「設定」

コンソールコマンドで設定する

本製品に直接コマンド（コンソールコマンド）を送って、本製品の機能を設定できます。TELNETまたはSSH経由で設定を変更するだけでなく、「かんたん設定ページ」からコンソールコマンドを入力して実行することもできます。TELNET、SSH経由で設定を変更する場合は、お使いの環境用のTELNETまたはSSHソフトウェアをご用意ください。

コンソールコマンドとは？

コンソールコマンドは、ルーターに直接命令を送って、機能を設定する方法です。コンソールコマンドを使うと、他の方法よりも、より詳しい設定が行えます。コンソールコマンドの詳細については、「コマンドリファレンス」（付属CD-ROMに収録）をご覧ください。

ヒント

本製品のCONSOLEポートにシリアルケーブルで接続したパソコンから、本製品をコンソールコマンドで設定することもできます（91ページ）。

TELNET、SSHで設定する

LANポートに接続しているパソコンからTELNETまたはSSHソフトウェアで本製品にログインし、コンソールコマンドを送信して設定します。

ご注意

コンソールコマンドは、コマンドの動作をよく理解した上でお使いください。「かんたん設定ページ」で設定後にコンソールコマンドで設定を変更すると、意図しない動作につながることがあります。設定後に意図した動作をするかどうか、必ずご確認ください。

ヒント

コンソールコマンドの詳細については、「コマンドリファレンス」（付属CD-ROMに収録）をご覧ください。

ユーザを登録する

「ユーザの追加」画面でTELNETまたはSSHでログインするユーザを登録します。TELNETでは、ユーザを登録しなくても無名ユーザとしてログインすることができますが、SSHでは登録ユーザでなければログインすることができません。

設定内容について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

「ユーザの追加」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」
▶「ユーザとアクセス制限の設定（HTTP、TELNET、SSH）」の「設定」
▶「ユーザとパスワードの設定」欄、「ユーザの登録数」の「設定」

SSHでログインできるように設定する

本製品のSSHサーバ機能は工場出荷状態では「使用しない」になっています。SSHでログインするためには、「ユーザとアクセス制限の設定」画面の「SSHサーバ機能」欄で設定を「使用する」に変更してください。

設定内容について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

「ユーザとアクセス制限の設定」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」

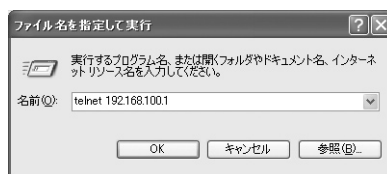
▶「ユーザとアクセス制限の設定(HTTP、TELNET、SSH)」の「設定」

TELNET、SSHで接続する

パソコンからの接続について、Windows標準のTELNETを使用する場合を例に説明します。SSHについてはご使用になるSSHソフトウェアの使用方法に従ってください。

1 **「スタート」メニューから「ファイル名を指定して実行」を選ぶ。**

2 **「telnet 192.168.100.1」と入力してから、「OK」をクリックする。**

本製品のIPアドレスを変更している場合には、「192.168.100.1」のかわりに本製品のIPアドレスを入力します。

3 **「Password:」と表示されたら、ログインパスワードを入力してからEnterキーを押す。**

何も表示されないときは、一度Enterキーを押します。

TELNETの場合、ここで入力するパスワードは、無名ユーザのログインパスワードです。無名ユーザとしてではなく、登録ユーザとしてログインするときは、何も入力せずにEnterキーのみを押すと「Username:」というプロン

プトが表示されます。同様に、既に無名ユーザでログインしているとき、または無名ユーザでのログインを禁止しているときは、最初から「Username:」というプロンプトが表示されます。
「Username:」に対し登録ユーザ名を入力すると「Password:」が表示されるので、登録ユーザのログインパスワードを入力してください。パスワードを設定していない無名ユーザでログインするときは、「Username:」とそれに続く「Password:」にともに何も入力せずEnterキーを押します。またSSHの場合は、無名ユーザでのログインはできないので、「Password:」に対し最初から登録ユーザのログインパスワードを入力します。
「>」が表示されると、コンソールコマンドを入力できるようになります。

```
Telnet 192.168.100.1

Password:

RT107e Rev.8.03.12 (Fri Jul  1 11:56:57 2005)
  Copyright (c) 1994-2005 Yamaha Corporation.
  Copyright (c) 1995-1996 Jean-loup Gailly and Mark Adler.
  Copyright (c) 1998-2000 Tokyo Institute of Technology.
  Copyright (c) 2000 Japan Advanced Institute of Science and Technology, HOKURIK
U.
  Copyright (c) 1997-2004 University of Cambridge. All rights reserved.
  Copyright (C) 1997 - 2002, Makoto Matsumoto and Takuji Nishimura, All rights r
eserved.
00:a0:de:07:f6:e6, 00:a0:de:07:f6:e7
Memory 32Mbytes, 2LAN
> administrator
Password:
#
#
# quit
> quit
```

ヒント

- 「help」と入力してからEnterキーを押すと、キー操作の説明が表示されます。
- 「show command」と入力してからEnterキーを押すと、コマンド一覧が表示されます。

4 **「administrator」と入力してから、Enterキーを押す。**

5 **「Password:」と表示されたら、管理パスワードを入力する。**

「#」が表示されると、各種のコンソールコマンドを入力できます。

6 **コンソールコマンドを入力して、設定する。**

7 **設定が終わったら、「save」と入力してからEnterキーを押す。**

コンソールコマンドで設定した内容が、本製品のメモリに保存されます。

8 **設定を終了するには、「quit」と入力してからEnterキーを押す。**

9 **コンソール画面を終了するには、もう一度「quit」と入力してからEnterキーを押す。**

「かんたん設定ページ」でコンソールコマンドを使用する

「コマンドの実行」画面で行います。

コンソールコマンドを入力してから「実行」をクリックすると、コマンドの実行結果が表示されます。
設定内容について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

「コマンドの実行」画面を開くには

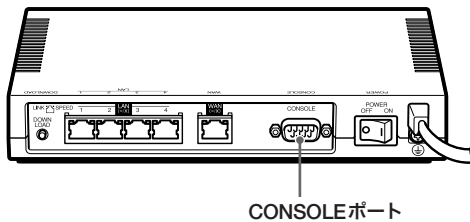
「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。
▶トップページの「詳細設定と情報」
▶「コマンドの実行」の「実行」

CONSOLEポートから設定する

本製品のCONSOLEポートにシリアルケーブルで接続したパソコンから、本製品をコンソールコマンドで設定できます。

- 「かんたん設定ページ」にパスワードを設定してTELNETでの設定を禁止しておけば(74ページ)、本製品の設定を変更できるのは本製品に物理的にアクセスできる立場のユーザーだけになり、セキュリティを強化するために役立ちます。
- 本製品に保存されている複数の設定ファイルから、どの設定で起動するのかをターミナルソフトウェアを使用してパソコンから指定することもできます。

CONSOLEポートとパソコンを接続する

本製品のCONSOLE ポートとパソコンのシリアルポートを、クロスタイプのシリアルケーブルで接続します。

ヒント

シリアルケーブルの両端のコネクタは、本製品(D-sub9ピン、オス)とパソコンに適合したタイプをご使用ください。

CONSOLEポート番号を確認する

接続に使用するパソコンのシリアルポートが、どのCOMポート番号に割り当てられているのかを確認します。

1 **「スタート」メニューから「マイ コンピュータ」をクリックする。**

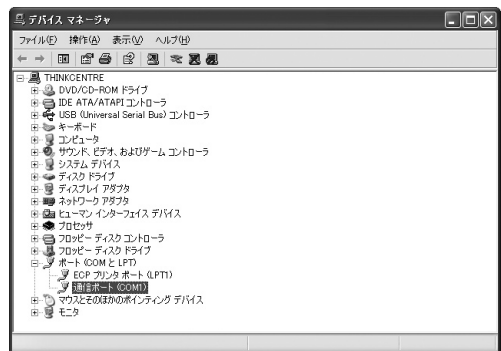
2 **「マイ コンピュータ」画面左側の「システムのタスク」欄にある、「システム情報を表示する」をクリックする。**

「システムのプロパティ」画面が表示されます。

3 **「ハードウェア」タブをクリックする。**

4 **「デバイス マネージャ」をクリックする。**

「デバイス マネージャ」画面が表示されます。

5 **「ポート(COMとLPT)」を展開して、「通信ポートのポート番号」(COMx)を確認する。**

通常は「COM1」が割り当てられています。

6 **「デバイス マネージャ」画面と「システムのプロパティ」画面を閉じる。**

CONSOLEポートを指定して接続する

CONSOLEポートに接続しているパソコンからターミナルソフトウェアで本製品にログインし、コンソールコマンドを送信して設定します。ここでは、Windows標準の「ハイパーターミナル」を使用する場合を例に説明します。

ご注意

コンソールコマンドは、コマンドの動作をよく理解した上でお使いください。「かんたん設定ページ」で設定後にコンソールコマンドで設定を変更すると、意図しない動作につながることがあります。設定後に意図した動作をするかどうか、必ずご確認ください。

ヒント

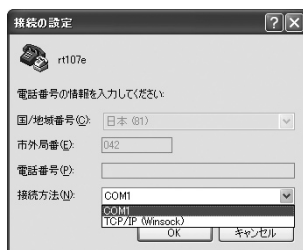
コンソールコマンドの詳細については、「コマンドリファレンス」（付属CD-ROMに収録）をご覧ください。

1 「スタート」メニューから「すべてのプログラム」–「アクセサリ」–「通信」–「ハイパーターミナル」をクリックする。

「接続の設定」画面が表示されます。

2 「名前」欄に接続名を入力する。

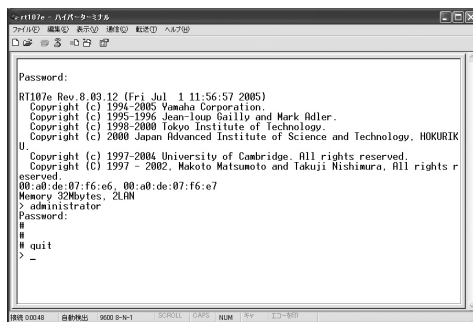
接続名は自由に設定してください。

3 「接続方法」で前ページで確認したパソコンのシリアルポート番号を選んでから、「OK」をクリックする。

「COMxのプロパティ」画面が表示されます。

4 通信設定を以下の値に変更する。

- ビット/秒：9600
- データビット：8
- パリティ：なし
- ストップビット：1
- フロー制御：Xon/Xoff

5 「OK」をクリックする。

ハイパーターミナルの画面が表示されます。

以後の操作は、「TELNET、SSHで接続する」（89ページ）の手順3以降と同じです。

本製品の起動時に設定ファイルを切り替える

本製品は設定ファイル(config)を最大5つ持つことができ、CONSOLEポートから設定する場合にのみそれらのファイルを切り替えることができます。

1 **本製品の電源を切る。**

2 **本製品のCONSOLEポートとパソコンのシリアルポートを、シリアルケーブルで接続する。**

接続については91ページ、パソコンの設定については91ページをご覧ください。

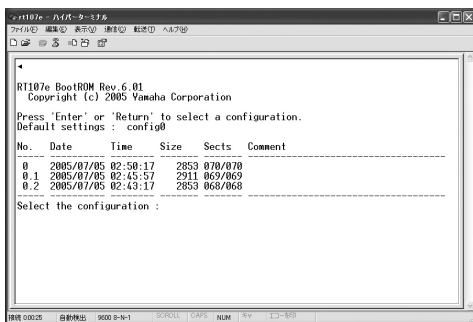
3 **パソコンでターミナルソフトウェアを起動する。**

詳しくは92ページをご覧ください。

4 **本製品の電源を入れる。**

パソコンのターミナルソフトウェアの画面に本製品のROMのバージョンが表示され、Enterキーの入力待ち状態になります。

5 **「Will start automatically in～ 」のカウントダウンが終わらないうちに、Enterキーを押す。**

設定ファイル待ち状態になります。

ヒント

「Will start automatically in～ 」のカウントダウンが終わると通常状態で起動してしまいます。起動してしまった場合は、本製品の電源を切ってから10秒以上の時間をおき、もう一度電源を入れ直して操作してください。

6 **0～4.2のうちで、使用したい設定ファイル名を指定してからEnterキーを押す。**

指定した設定ファイルを使用して、本製品が起動します。

ご注意

- 本製品の電源を入れ直す場合には、電源を切ってから再度電源を入れるまでの間に、10秒以上の時間をおいてください。
- CONSOLEポートにパソコンが接続されていない場合や、接続されていてもパソコンからのキー入力が無い場合には、10秒後にデフォルト設定ファイルで自動的に起動します。
  - 工場出荷設定では、設定ファイル0で起動します。
  - set-default-configコマンドが設定されている場合は、指定されたデフォルト設定ファイルで起動します。
  - デフォルト設定ファイルが存在しない場合は、「何も設定されていない」状態で起動します。

設定ファイルを管理する

saveコマンドと設定ファイルの関係

本製品は5個の設定ファイル（config0～config4）を内蔵の不揮発性メモリに保持して、起動時に切り替えて使用できます。また、これらの設定ファイルには最大2個の退避ファイル（「configX.1」および「configX.2」と表示されるバックアップファイル）を保持できます。
退避ファイルは、saveコマンドを実行するごとに自動生成されます。saveコマンドを実行する場合には、現在動作中の設定ファイルの系列を把握しておくよう、ご注意ください。

例:config1で動作中にsaveコマンドを実行した場合の動作

- 不揮発性メモリ上のconfig1の内容が退避ファイルconfig1.1となります。
- 現在の動作環境設定がconifg1に上書きされます。
- config1.1がすでに存在する場合は、config1.1の内容はconfig1.2に上書きされます。
  config1.2がすでに存在する場合は、saveコマンド実行に伴ってconfig1.2の内容は破棄されます（config1.1の内容で上書きされます）。

ヒント

- 現在動作中の設定ファイルの番号を知りたい場合には、show environmentコマンドを実行します。
- すべての設定ファイルと退避ファイルの一覧を表示させるには、show config listコマンドを実行します。

設定ファイルを途中で切り替えたい場合は

restartコマンドを実行して本製品の起動プロセスに戻ってから、起動に使用する設定ファイルを選択できます。

ご注意

現在の動作環境が不揮発性メモリに保存されていない場合は、restartコマンド入力時に設定を保存するかどうか確認を求められます。ここで設定を保存すると、saveコマンド実行時と同様に退避ファイルが生成・上書きされます。

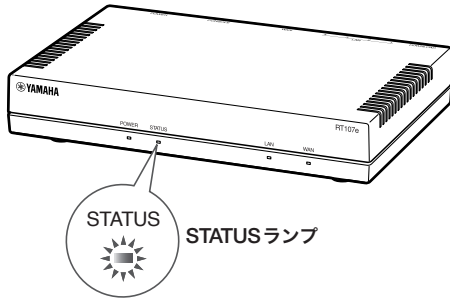
通常使用する設定ファイルを指定することもできます

set-default-configコマンドを使用して、起動プロセスにおいて設定ファイルを指定しない場合に自動選択される設定ファイル（デフォルト設定ファイル）を指定できます。TELNETで本製品にアクセスしている場合は起動プロセスで設定ファイルを指定できませんので、特定の設定ファイルで起動させたいときはこのコマンドを使用します。

ご注意

- デフォルト設定ファイルとして退避ファイルを指定している場合は、起動後にsaveコマンドを実行すると現在の動作環境が設定ファイルに上書きされてしまいます。必要であれば、使用したい設定ファイルの内容を別の設定ファイルにコピーしてから、saveコマンドを実行するようにしてください。
- 設定ファイル、退避ファイルを別の番号系列の設定ファイルに保存または削除する場合には、copy config、delete configコマンドを使用します。詳しくは「コマンドリファレンス」（付属CD-ROMに収録）をご覧ください。

STATUSランプで通信状態を確認する

各接続設定でキープアライブ機能を有効にしている場合は、接続先の機器との通信が不可能な状態になっているかどうか、本製品のSTATUSランプで確認できます。

「かんたん設定ページ」のトップページを表示せずに通信状態を確認できるので便利です。

ヒント

- 「かんたん設定ページ」からプロバイダとの接続やIPsecによるVPN接続、IPIPによるトンネル接続を設定する場合は、初期設定画面のキープアライブ機能は「有効」になっています。
- キープアライブが有効になっているかどうかを確認するには、それぞれの接続の設定画面をご覧ください。

「PPPoEを用いる端末型ADSL接続(フレッツ・ADSL、Bフレッツ」接続の設定画面の例

STATUSランプが点灯しているときは

キープアライブ機能を有効に設定した接続設定において、接続先の機器との通信が不可能な状態になっています。

ご注意

- キープアライブ機能は通信が不可能な状態を検出するまでに時間がかかります。そのため、STATUSランプが点灯していない状態でも、接続先の機器と通信ができない場合があります。
- DOWNLOADボタンからファームウェアのリビジョンアップを実行した場合も、STATUSランプは点灯します。DOWNLOADボタンからリビジョンアップを行った時の動作については「DOWNLOADボタンでリビジョンアップする」(次ページ)をご覧ください。

問題が解消すると

STATUSランプは消灯します。

最新の機能を利用する(リビジョンアップ)

インターネットから本製品の機能を管理するプログラム(ファームウェア)をダウンロードして、最新の機能をご利用いただけます(リビジョンアップ)。

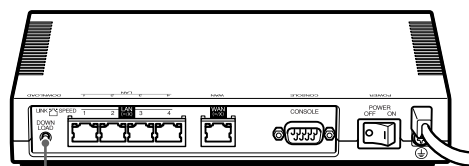
ご注意

- リビジョンアップを始めたら、完了して本製品が再起動するまで他の操作は絶対しないでください。万一、中断したときは本製品が使えなくなることがあります。その場合は、持ち込み修理が必要となります。
- リビジョンアップ中は、STATUS、LAN、WANランプが順番に点灯します。
- リビジョンアップが完了すると、本製品は自動的に再起動されるため、すべての通信が切断されます。
- リビジョンアップ中は、絶対にケーブルを抜かないでください。ルーターが使えなくなり、持ち込み修理が必要となる場合があります。
- 「かんたん設定ページ」の「リビジョンアップの実行」画面では、正式にリリースされたバージョンのファームウェアにのみリビジョンアップできます。ヤマハによる正式な動作保証のないβ版のファームウェアは、「かんたん設定ページ」を使ってリビジョンアップすることはできません。

ヒント

「かんたん設定ページ」の「リビジョンアップの実行」画面で、「リビジョンダウンの許可」を「許可する」に変更すると、リビジョンダウン(旧バージョンのファームウェアに更新)も実行できます。詳しくは「リビジョンアップの実行」画面のヘルプをご覧ください。

DOWNLOADボタンでリビジョンアップする

「DOWNLOADボタンの設定」画面でリビジョンアップを「許可する」に設定している場合は、本製品背面のDOWNLOADボタンを3秒間押し続けることで、リビジョンアップを実行できます。

DOWNLOADボタン

ヒント

DOWNLOADボタンでリビジョンアップを実行する場合、本製品のランプでリビジョンアップの状態を確認できます。

- ファームウェアをダウンロードしている間は、STATUSランプが点滅します。
- ファームウェアのダウンロードが完了して、リビジョンアップが開始されると、STATUS、LAN、WANランプが順番に点灯します。
- ダウンロードやリビジョンアップに失敗した場合は、STATUSランプが点灯します。DOWNLOADボタンを1秒間押して、点灯を解除してください。

DOWNLOADボタンによるリビジョンアップを許可する

「DOWNLOADボタンの設定」画面で行います。

DOWNLOADボタンによるリビジョンアップを行いたいときは、「許可する」を選びます。
設定内容について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

「DOWNLOADボタンの設定」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。
▶トップページの「詳細設定と情報」
▶「DOWNLOADボタンの設定」の「設定」

DOWNLOADボタンを押してリビジョンアップする

DOWNLOADボタンを押すと、新しいリビジョンのファームウェアの有無をチェックします。新しいリビジョンのファームウェアがあった場合は、自動的にファームウェアをダウンロードしてから、リビジョンアップを実行します。

ご注意

- ファームウェアのダウンロードまたはリビジョンアップに失敗すると、STATUSランプが点灯します。その場合はDOWNLOADボタンを1秒間押すと、STATUSランプが消灯します。
- ファームウェアのダウンロード、またはリビジョンアップに失敗した場合は、「Q6 DOWNLOADボタンが機能しない」(108ページ)をご確認ください。

リビジョンアップが終了すると

本製品が再起動します。

「かんたん設定ページ」でリビジョンアップする

「リビジョンアップの実行」画面で行います。

「実行」をクリックすると、新しいリビジョンのファームウェアの有無をチェックします。新しいリビジョンのファームウェアがあった場合は、画面に今のリビジョン番号と新しいリビジョン番号が表示されます。その状態でもう一度「実行」をクリックすると、ファームウェアのダウンロード後に自動でリビジョンアップを実行します。
設定内容について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

ヒント

「リビジョンアップの実行」画面で「リビジョンダウンの許可」を「許可する」に変更すると、リビジョンダウン(旧バージョンのファームウェアに更新)も実行できます。

「リビジョンアップの実行」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。
▶トップページの「詳細設定と情報」
▶「リビジョンアップの実行」の「実行」

リビジョンアップが終了すると

本製品が再起動します。
本製品の「かんたん設定ページ」にアクセスして、リビジョン番号が更新されていることを確認してください。

本製品の設定情報とログを確認する

本製品の設定情報を確認する

プロバイダに接続するために必要な情報や各種の設定情報は、本製品の内部で1つの設定ファイル(config)として管理されています。この設定ファイルをパソコンに保存すると、設定のバックアップとして利用したり、設定ファイルをパソコンで編集したりできるので便利です。また、サポート窓口にお問い合わせいただく場合にも、設定ファイルの内容がわかった方がトラブルの早期解決につながることがあります。

1 「かんたん設定ページ」のトップページで「詳細設定と情報」をクリックしてから、「本製品の全設定(config)のレポート作成」の「実行」をクリックする。

「本製品の全設定(config)のレポート作成」画面に本製品の全設定情報が表示されます。

2 表示された設定情報をコピーして、「メモ帳」などのソフトウェアに貼り付けて保存する。

ヒント

パソコンで編集した設定ファイルを本製品に転送したいときは、あらかじめテキスト形式の設定ファイルの内容をクリップボードにコピーしておいてから、「コマンドの実行」画面(90ページ)に貼り付けます。

本製品のログを確認する

本製品の動作履歴は、ログファイル(syslog)として管理されています。ログファイルで本製品の動作履歴を確認することで、ネットワークの障害を解決するヒントになる場合があります。

ご注意

本製品の電源を切った場合には、ログファイルの内容は全て消去されます。

ヒント

ログファイルの保存方式には、いくつかの段階があります。詳しくは「コマンドリファレンス」(付属CD-ROMに収録)をご覧ください。

1 「かんたん設定ページ」のトップページで「詳細設定と情報」をクリックしてから、「本製品のログ(syslog)のレポート作成」の「実行」をクリックする。

「本製品のログ(config)のレポート作成」画面に本製品のログが表示されます。

2 表示されたログをコピーして、「メモ帳」などのソフトウェアに貼り付けて保存する。

ルーターの運用管理

故障かな？ と思ったら

お問い合わせになる前に

本書の内容をご覧になり、問題を解決してみましょう。

基本的なチェック

- **POWERランプは点灯していますか？**
  点灯していない場合は、次ページをご覧ください。
- **WANランプは点灯していますか？**
  点灯していない場合は、次ページをご覧ください。
- **LANランプは点灯していますか？**
  点灯していない場合は、次ページをご覧ください。

STATUSランプの状態を確認してください

点灯している場合は、通信に障害が発生しています。95ページをご覧ください。

問題を解決する

症状ごとの説明ページをご覧ください。

それでも問題が解決しない場合は

サポート窓口までご相談ください（113ページ）。

Q1 ランプ類が消灯している

症状▶	原因▶	対策
ランプがひとつも点灯しない	本製品の電源が入っていない	POWER（電源）スイッチを「ON」にして、電源を入れる。
	電源コードがコンセントに接続されていない	コンセントから外れているときは、正しく差し込み直す。
	主ブレーカーや配線別ブレーカーが切れている	• ブレーカーが「切」になっている場合は、「入」にする。 • ブレーカーが「入」になっている場合は、一度「切」にしてから「入」にし直す。
	停電している	停電中は、復旧するまでお待ちください。
	コンセントに電気が来ていない（他の電気製品も使えない）	• 他の製品が動かないときは、コンセントや電気配線の修理を依頼してください。 • 他の製品が動くときは、本製品の修理を依頼してください。
LANランプが点灯しない	HUBやパソコンの電源が入っていない	本製品および本製品に接続した機器の電源が入っていることを確認する。LANポートに機器を正しく接続しても、接続した機器の電源が入っていないときは、本製品のLANランプは点灯しない。
	正しく接続されていない	本製品側、パソコンおよびHUB側共にコネクタをいったん外してから、もう一度カチッとロックするまで差し込む。
	LAN用のケーブルを使っていない	• ISDNケーブルを使用していないかどうか確認する（コネクタ形状が全く同じなので注意が必要）。 • 他のLANケーブルと取り替えてみる。
	パソコンのLAN（ネットワーク）カードが正しく動作していない、または接続モードが本製品と合っていない	• 他の製品が動かないときは、コンセントや電気配線の修理を依頼してください。 • 他の製品が動くときは、本製品の修理を依頼してください。
WANランプが点灯しない	ADSLモデムやケーブルモデム、ONUの電源が入っていない	電源を入れる。
	ADSLモデムやケーブルモデム、ONUと正しく接続されていない	本製品のWANポートおよびADSLモデムやケーブルモデム、ONUの配線をいったん外してから、もう一度カチッと音がするまで差し込む。
	正しいケーブルを使用していない	ADSLモデムやケーブルモデム、ONUとパソコンを接続するものと、同じタイプのケーブルで接続する。

Q2 「かんたん設定ページ」で設定できない

症状	原因	対策
「かんたん設定ページ」を表示できない	本製品がパソコンを認識していない(LANランプが点灯していない)	「LANランプが点灯しない」(前ページ)の説明に従って、問題を解決する。
	パソコンのネットワーク設定が不適切(LAN上の他のパソコンやネットワークプリンタも使用できない)	• LANボードやLANカードの設定をやり直して、パソコンを再起動する。 • IPアドレスをリセットする(32ページ)。
	本製品が誤動作している	本製品を初期状態に戻してから、設定をやり直す(110ページ)。
	本製品のIPアドレスを変更した	• 本製品に設定したIPアドレス「http://(本製品のIPアドレス）/」にアクセスする。 • 本製品とLANに接続しているすべてのパソコンを再起動する。再起動または電源を切ることができないときは、パソコンを1台だけ本製品に接続し、それ以外のLANケーブルを取り外してから、本製品とパソコンの電源を入れる。 • パソコンの設定が同じIPアドレス範囲になっているか、他の機器とIPアドレスが重なっていないか確認する。
	ルータのURLが不適切である	本製品を初めて使うときや工場出荷状態に戻した後は、「http://192.168.100.1/」にアクセスする。
	パソコンのWebブラウザの接続経路設定が、LAN経由になっていない	Windows版InternetExplorer6 の場合、「インターネットオプション」の「接続」タブでダイヤルアップ接続をする設定になっていると、「かんたん設定ページ」にアクセスできないので、「ダイヤルしない」に変更する。
	パソコンのWebブラウザでProxy（プロキシ）サーバを使用している	• プロキシの設定が正しくないと、「かんたん設定ページ」が表示できなくなる。 • Windows版InternetExplorer6の場合：メニューから「ツール」→「インターネットオプション」→「接続」タブ→「LANの設定」を開き、「プロキシサーバーを使用する」のチェックをはずす。

Q2 「かんたん設定ページ」で設定できない(つづき)

症状	原因	対策
「かんたん設定ページ」を表示できない(つづき)	パソコンをWebブラウザ経由で遠隔操作している	• IPアドレスによるアクセス制限機能が働いていると、許可されていないホストからのアクセスに対しては、「Error503 This server is available to membersonly. I'm sorry, your host is notmember.」と表示される。遠隔操作する場合は、「HTTPの利用を許可するホスト」の設定を変更する(74ページ)。
パスワードを入力しても「かんたん設定ページ」が表示されない	パスワードが間違っている(パスワードエラーが表示される)	• パスワードは、全角/半角や大文字/小文字の違いも区別される。必ず半角の英数字で大文字/小文字まで正確に入力する。 • Webブラウザに認証情報(ユーザ名、パスワード)が残っていると、それを自動的に送信するため、エラーになる場合がある。ユーザ名を削除してからパスワードを入力し直すか、ブラウザをいったん終了してから「かんたん設定ページ」を開き直す。
	ログインパスワードでは「かんたん設定ページ」にアクセスできない	パスワードを設定している場合は、管理パスワードを入力する。
設定内容が元に戻ってしまう	設定後に「設定の確定」をクリックしていない	「かんたん設定ページ」で設定を変更したときは、必ず「設定の確定」をクリックして設定を保存する。「設定の確定」をクリックせずに「トップに戻る」をクリックしたり画面を閉じたりすると、設定内容は保存されない。
「かんたん設定ページ」を開く際に、Webブラウザにパスワードを保存できない	「ネットワークパスワードの入力」画面で、ユーザ名を空欄にしている	Webブラウザによっては、パスワードを保存するためにユーザ名の入力が必要な場合がある。この場合は、任意の文字列を入力する。

Q3 インターネットに接続できない

症状	原因	対策
フレッツ・ADSLやBフレッツで接続できない	本製品がブロードバンド回線を認識していない（WANランプが点灯していない）	「WANランプが点灯しない」（100ページ）の説明に従って、問題を解決する。
	ユーザIDまたはパスワードが間違っている	• プロバイダから指定されたユーザIDに加えて、プロバイダ名まで指定する必要がある（例:username@xxx.ne.jp）。 • フレッツ・ADSL（またはBフレッツ）とプロバイダの設定資料を参照して、正しく入力する。
ホームページが表示されない／表示が遅い	プロバイダ設定のDNSサーバアドレスが間違っている	• プロバイダ接続設定にDNSサーバアドレスが設定されているか確認する。 • 各パソコンのDNSサーバアドレス設定に本製品のIPアドレスを入力してから、パソコンを再起動する。 • WebサーバやDNSサーバが混雑または停止している可能性がある。しばらく時間をおいてから、アクセスし直す。
	本製品のフィルタが動作している	プロバイダから与えられたIPアドレスがプライベートアドレスで、ファイアウォールなどのセキュリティフィルタを適用している場合は、セキュリティレベルを2か4、または6に変更する（70ページ）。
	回線の種類に問題がある（PPPoE方式ADSL接続時のみ）	ADSL回線の種類によっては、標準的な設定のままでは、一部のホームページのデータが受信できないか、データの受信が非常に遅くなることがある。 いったん接続を切断してから、「かんたん設定ページ」の「詳細設定と情報」－「基本接続の詳細な設定」－「プロバイダの登録/修正」画面でMTUに1454などの値を設定して、接続し直す。
	プロバイダから与えられたIPアドレスと本製品に設定したIPアドレスが重複している	「かんたん設定ページ」の「LANの設定」画面で、本製品のIPアドレスをプロバイダから与えられたものと重複しないアドレスに変更する（30ページ）。この場合、本製品のファイアウォール機能は再適用する必要がある。

Q3 インターネットに接続できない（つづき）

症状▷	原因▷	対策
ホームページが表示されない/表示が遅い（つづき）	パソコンのネットワーク設定が不適切	• LANボードやLANカードの設定をやり直して、パソコンを再起動する。 • IPアドレスをリセットする（32ページ）。
	回線やプロバイダ、Webサーバが混雑している	時間帯などによっては、非常に遅くなる場合がある。回線速度に比べて非常に遅い状態が続く場合は、ご利用の回線業者やプロバイダにお問い合わせください。

Q4 VPN通信ができない

症状	原因	対策
「かんたん設定ページ」のトップページでIPsecトンネル接続が「通信中」と表示されない	インターネットに接続していない	● インターネットに接続する設定を行っているかを確認する。 ● 「Q3 インターネットに接続できない」(103ページ)の説明に従って、問題を解決する。
	IPsec接続の接続先と通信ができない	IPsecの接続先のIPアドレスに対してpingコマンドを実行して、応答が返ってくるかどうかを確認する。応答が返ってこなければ、接続先の機器が通信可能な状態になっているかを確認する。
IPsec接続のVPN通信ができない	IPsec接続が確立していない	● IPsecの接続先と同じ認証鍵(pre-shared key)を設定しているかを確認する。 ● 接続先の識別方法で、正しいIPアドレスまたは正しい名前を設定しているかを確認する。 ● IPsecの接続先と同じ認証アルゴリズム、暗号アルゴリズムを設定しているかを確認する。
	経路情報が誤って設定されている	経路情報に接続先のLANのネットワークアドレスを正しく設定する。
	接続先のLAN内に設置されているパソコンの設定が誤っている	● 通信に使用するアプリケーションソフトウェアの設定を確認する。 ● パソコンのファイアウォール機能が有効になっている場合には、通信に使用されているパケットをブロックしないように、ファイアウォール機能の設定を変更する。 WindowsXPでは、「スタート」-「ヘルプとサポート」をクリックして表示される画面で、「検索」欄に「ファイアウォール」を入力して検索すると関連する情報が表示されるので、その内容に従って問題を解決する。
IPsec接続のVPN通信が遅い	インターネットの通信が遅い	「Q3 インターネットに接続できない」(103ページ)の説明に従って、問題を解決する。

Q4 VPN通信ができない(つづき)

症状	原因	対策
「かんたん設定ページ」のトップページでIPIPトンネル接続が「通信中」と表示されない	フレッツ網に接続していない	フレッツ網に接続する設定を行っているかを確認する。
	IPIPトンネル接続の接続先と通信ができない	IPIPトンネルの接続先のIPアドレスに対してpingコマンドを実行して、応答が返ってくるかどうかを確認する。応答が返ってこなければ、接続先の機器が通信可能な状態になっているかを確認する。
IPIPトンネル接続のVPN通信ができない	IPIPトンネル接続が確立していない	● 接続先のIPアドレスに、フレッツ網から接続先に払い出されたIPアドレスが正しく設定されているかを確認する。 ● 「かんたん設定ページ」の「詳細設定と情報」-「VPN接続の設定」のIPIPトンネル接続の設定画面で、「接続プロバイダ」にフレッツ網との接続に使用されているインタフェースが選択されているかを確認する。
	経路情報が誤って設定されている	経路情報に接続先のLANのネットワークアドレスを正しく設定する。
	接続先のLAN内に設置されているパソコンの設定が誤っている	● 通信に使用するアプリケーションソフトウェアの設定を確認する。 ● パソコンのファイアウォール機能が有効になっている場合には、通信に使用されているパケットをブロックしないように、ファイアウォール機能の設定を変更する。 WindowsXPでは、「スタート」-「ヘルプとサポート」をクリックして表示される画面で、「検索」欄に「ファイアウォール」を入力して検索すると関連する情報が表示されるので、その内容に従って問題を解決する。
IPIPトンネル接続のVPN通信が遅い	フレッツ網の通信が遅い	回線状態に問題がないかを回線事業者にお問い合わせください。

Q5 STATUSランプが機能しない

症状	原因	対策
通信障害が発生していないのにSTATUSランプが点灯している	DOWNLOADボタンによるリビジョンアップが行われている	リビジョンアップが完了した後に、再度STATUSランプを確認する。
通信障害が発生しているのにSTATUSランプが点灯しない	キープアライブ機能が有効になっていない	プロバイダ接続やVPN接続の設定で、キープアライブ機能が有効になっているかを確認する。
	キープアライブ機能が通信障害を未だ検出していない	数分間待ってから、再度STATUSランプを確認する。
	PPPoE接続が「かんたん設定ページ」の「切断」のクリックにより切断された	「かんたん設定ページ」の「接続」をクリックして接続し直す。
	PPPoE接続が切断タイマによって切断された	タイマで自動切断しないように設定を変更する。
STATUSランプの点灯を解除できない	通信障害から復旧していない	「Q3 インターネットに接続できない」(103ページ)、「Q4 VPN通信ができない」(105ページ)の説明に従って、問題を解決する。

Q6 DOWNLOADボタンが機能しない

症状▷	原因▷	対策
DOWNLOADボタンを押してもリビジョンアップされない	インターネットに接続していない	インターネットに接続する設定を行っているかを確認する。「Q3 インターネットに接続できない」(103ページ)の説明に従って、問題を解決する。
	ファームウェアのダウンロード先URLの設定が間違っている	「かんたん設定ページ」の「詳細設定と情報」–「リビジョンアップの実行」画面で「ダウンロードするURL」を正しく設定する。
	DOWNLOADボタンの使用を許可する設定になっていない	「かんたん設定ページ」の「詳細設定と情報」–「DOWNLOADボタンの設定」画面で「リビジョンアップの許可」を「許可する」に設定する。
	最新リビジョンのファームウェアを使用している	そのまま使い続けてください。
STATUSランプが点滅し始めた	ファームウェアをサーバーからダウンロードしている(正常な状態)	そのままの状態でお待ちください。ケーブルを抜いたり、電源を切ったりしないでください。
STATUS、LAN、WANランプが順番に点灯し始めた	ファームウェアを不揮発性メモリに書き込んでいる(正常な状態)	そのままの状態でお待ちください。ケーブルを抜いたり、電源を切ったりしないでください。
STATUSランプが点灯したままの状態になった	リビジョンアップに失敗した	「DOWNLOADボタンを押してもリビジョンアップされない」(本ページ)の説明に従って、問題を解決する。 STATUSランプの点灯を解除する場合は、DOWNLOADボタンを1秒間押す。
DOWNLOADボタンを1秒間押しても、STATUSランプが消灯しない	通信障害が発生している	「Q5 STATUSランプが機能しない」(前ページ)の説明に従って、問題を解決する。

Q7 その他の問題

症状	原因	対策
本製品やパソコンで、NTPサーバを使った時刻合わせができない	NTPサーバのIPアドレスやドメイン名が間違っている	• 入手したNTPサーバ情報と比較し、正しく設定されていることを確認する。 • NTPサーバに対してpingを実行し、NTPサーバが稼動していることを確認する。
	登録されているNTPサーバへの経路が設定されていない	プロバイダ設定や経路設定を確認する。
	本製品のセキュリティフィルタが動作している	1 「かんたん設定ページ」の「詳細設定と情報」-「ファイアウォール設定」-「IPv4ファイアウォールの設定」画面で、「静的フィルタの一覧」の下部に表示されているNTPポート（ポート番号123）を通す（Pass）フィルタ（36 / 37番）の「入」と「出」の両方にチェックを付ける。 2 セキュリティレベルを6または7にする（70ページ）。
ネットボランチDNSサービスでホストアドレスを取得できない	プロバイダによっては、登録／更新してすぐに名前解決ができない場合がある	しばらく時間をおいてから、再度試してみる。
	ネットワーク型プロバイダ接続で接続している	ネットワーク型プロバイダ接続で接続している場合は、ネットボランチDNSサービスは利用できない。IPアドレスを直接指定して接続する。
	プロバイダからプライベートIPアドレスが割り当てられている	本製品にグローバルIPが割り当てられていない環境では、ネットボランチDNSサービスは利用できない。

本製品の設定を初期化する

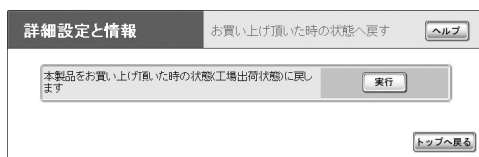
本製品の設定内容を工場出荷状態に戻すことができます。

ご注意

設定内容を工場出荷時の状態に戻す場合は、以下の点にご注意ください。

- 実行した直後にすべての通信が切断されます。
- 初期設定値が存在する設定は、初期設定値に変更されます。
- フィルタ定義や登録されたアドレスは消去されます。
- saveコマンドなしで、不揮発性メモリの内容が書き換えられます。
- 操作を完了した後に、設定内容を元の状態に戻すことはできません。

「かんたん設定ページ」から初期化する

本製品の設定内容を工場出荷状態に戻したいときは、「お買い上げ頂いた時の状態へ戻す」画面で設定を初期化できます。

設定内容について詳しくは、設定画面の「ヘルプ」をクリックして、表示される説明をご覧ください。

「お買い上げ頂いた時の状態へ戻す」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」

▶「お買い上げ頂いた時の状態へ戻す」の「実行」

「かんたん設定ページ」から初期化できないときは

本製品のIPアドレスを誤って設定した場合など、本製品の「かんたん設定ページ」から初期化できない場合には、CONSOLEポートに接続したパソコンを使用して本製品を初期化できます。

1 **本製品の電源を切る。**

2 **本製品のCONSOLEポートとパソコンのシリアルポートを、シリアルケーブルで接続する。**

接続については91ページ、パソコンの設定については91ページをご覧ください。

3 **パソコンでターミナルソフトウェアを起動する。**

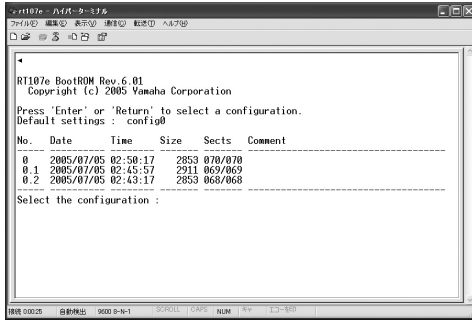
詳しくは92ページをご覧ください。

4 **本製品の電源を入れる。**

パソコンのターミナルソフトウェアの画面に本製品のROMのバージョンが表示され、Enterキーの入力待ち状態になります。

5 **「Will start automatically in～ 」のカウントダウンが終わらないうちに、Enterキーを押す。**

「Will start automatically in～ 」のカウントダウンが終わると通常状態で起動してしまいます。起動してしまった場合は、本製品の電源を切ってから10秒以上の時間をおき、もう一度電源を入れ直して操作してください。

6 **設定ファイルの選択待ち状態になったら、0～4.2のうちで表示されていない設定ファイルを指定してからEnterキーを押す。**

ファームウェアが起動すると、ファームウェアのリビジョンなどが表示されます。

7 **10秒程度待ってから、Enterキーを押す。**

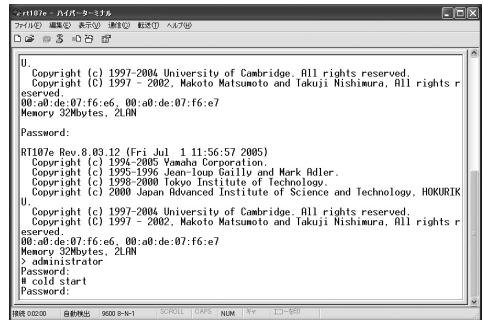
8 **「Password:」と表示されたら、Enterキーを押す。**

「>」が表示されると、コンソールコマンドを入力できるようになります。

9 **「administrator」と入力してから、Enterキーを押す。**

10 **「Password:」と表示されたら、Enterキーを押す。**

11 **「#」が表示されたら、「cold start」と入力してからEnterキーを押す。**

12 **「Password:」と表示されたら、Enterキーを押す。**

本製品の設定が初期化されます。

パスワードを忘れてしまった場合は

ログインパスワードや管理パスワードとして設定した文字列を忘れてしまうと、本製品にログインできなくなります。このような場合でも、CONSOLEポートに接続したシリアル端末から以下の非常用パスワードを入力すると、本製品にログインできます。

非常用パスワード
「w,lXlma」(ダブリュ -、カンマ、エル、エックス、エル、エム、エー)

ヒント
CONSOLEポートへの接続については91ページ、パソコンの設定については91ページをご覧ください。

非常用パスワードを使ってログインすると最初から管理モードに入れますので、忘れてしまったログインパスワードや管理パスワードを再設定してください。パスワード設定の際に要求される古いパスワードも、この非常用パスワードが利用できます。

ご注意
- この機能は、security classコマンドの設定で禁止することもできます。詳しくは「コマンドリファレンス」(付属CD-ROMに収録)をご覧ください。
- security classコマンドの第2パラメータで「on」が指定されていない場合は、この方法でもログインできません。

サポート窓口のご案内

お問い合わせの前に

本書をもう一度ご確認ください

本書をよくお読みになり、問題が解決できるかどうかご確認ください。

ログ情報や設定情報をご確認ください

お客様のルータの状態を把握するために、弊社の担当者がログ(Syslog)情報や設定(config)情報を確認させていただくことがあります。ログ情報や設定情報を問題の症状とあわせてお知らせいただくことで、問題の解決が早まることがあります。ログ情報や設定情報は、以下の方法でご確認ください。

1 パソコンでWebブラウザを起動して、ファイルメニューの「開く」を選ぶ。

「ファイルを開く」画面が表示されます。

2 「http://192.168.100.1/」と半角英字で入力してから、「OK」をクリックする。

トップページが表示されます。

3 「詳細設定と情報」をクリックする。

詳細設定と情報」画面が表示されます。

4 ログ情報を確認したいときは「本製品のログ(Syslog)のレポート作成」、設定情報を確認したいときは「本製品の全設定(config)のレポート作成」の「実行」をクリックする。

本製品のログ表示または全設定情報が表示されます。

「本製品の設定情報とログを確認する」(98ページ)もあわせてご覧ください。

お問い合わせ窓口

本製品に関する技術的なご質問やお問い合わせは、下記へご連絡ください。

ヤマハルーターお客様ご相談センター

TEL：053-478-2806
FAX：053-460-3489
ご相談受付時間
9:00~12:00 13:00~17:00
(土・日・祝日、弊社定休日、年末年始は休業とさせて頂きます。)
お問い合わせページ
http://NetVolante.jp/
http://www.rtpro.yamaha.co.jp/

主な仕様

外形寸法(幅×高さ×奥行き):
220 mm×42.6 mm×141.5 mm

質量:
700 g

電源:
AC100 V(50/60 Hz)

消費電流:
最大0.09A

動作環境条件:
周囲温度 0〜40 ℃
周囲湿度 15〜80 %(結露しないこと)

保管環境条件:
周囲温度 ー 20〜50 ℃
周囲湿度 10〜90 %(結露しないこと)

電波障害規格:
VCCI クラスA

認証番号:
D05-0292001

LANインタフェース:
イーサネット 10BASE-T/100BASE-TX
4ポートスイッチングHUB
プロトコル:IEEE802.3/IEEE802.3u
通信モード:オートネゴシエーション、固定設定
コネクタ:RJ-45
MACアドレス:本製品ラベルに表示
極性:ストレート/クロス自動判別

WANインタフェース:
イーサネット 10BASE-T/100BASE-TX
1ポート
プロトコル:IEEE802.3/IEEE802.3u
通信モード:オートネゴシエーション、固定設定
コネクタ:RJ-45
MACアドレス:本製品ラベルに表示
極性:ストレート/クロス自動判別

シリアルインターフェース
DTE固定
(パソコンとの接続はクロスケーブル)
ポート数:1
非同期シリアル:RS-232C
コネクタ:D-sub 9ピン
データ転送速度:9600bit/s
データビット長:8ビット
パリティチェック:なし
ストップビット数:1ビット
フロー制御:ソフトウェア(Xon/Xoff)

表示機能(LED)
前面:POWER、STATUS、LAN、WAN
背面:LINK、SPEED

付属品:
LANケーブル(3 m、RJ-45、ストレート)(1本)
取扱説明書(本書)(1冊)
CD-ROM(1枚)
保証書(1枚)

本製品を譲渡／廃棄する際のご注意

本製品を譲渡／廃棄する際は、以下の操作を行ってください。

1.ネットボランチDNSの登録を削除する

2.設定内容を初期化する

ご注意

- 先に設定内容を初期化してしまうと、ネットボランチDNSサーバに登録されたホストアドレスを削除できなくなります。必ずネットボランチDNSの登録を削除してから、設定内容を初期化するようにしてください。
- ネットボランチDNSの登録の削除は、ネットボランチDNS（ホストアドレスサービス)を登録したお客様のみ行ってください。
- 本製品を譲渡する際は、付属のマニュアル類もあわせて譲渡してください。

ネットボランチDNSの登録を削除する

ネットボランチDNSサービスを効率良く運用するために、譲渡／廃棄前に不要となったネットボランチDNSの登録の削除にご協力ください。

「ネットボランチDNSホストアドレスサービスの設定」画面で、「削除」をクリックします。

「ネットボランチDNSホストアドレスサービスの設定」画面を開くには

「かんたん設定ページ」から、以下の順に設定画面のボタンをクリックします。

▶トップページの「詳細設定と情報」

▶「ネットボランチDNSホストアドレスサービスの設定」の「設定」

設定内容を初期化する

保存されている設定内容には、プロバイダへの接続に必要なIDやパスワードも含まれています。設定内容を初期化せずに譲渡／廃棄すると、これらの情報が悪意のある第三者によって悪用されるおそれがあります。

初期化のしかたについては、「本製品の設定を初期化する」(110ページ)をご覧ください。

索引

英数字

五十音順

ア行

カ行

サ行

タ行

ナ行

ハ行

ラ行